UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE DIREITO

CURSO DE GRADUAÇÃO EM DIREITO

CLARISSA NOGUEIRA JOSINO

DADOS PESSOAIS, SEGURANÇA PÚBLICA E INVESTIGAÇÃO CRIMINAL: UM PANORAMA DA PROTEÇÃO DE DADOS E SEUS DESAFIOS REGULATÓRIOS NO BRASIL

FORTALEZA, 2021

CLARISSA NOGUEIRA JOSINO

DADOS PESSOAIS, SEGURANÇA PÚBLICA E INVESTIGAÇÃO CRIMINAL: UM PANORAMA DA PROTEÇÃO DE DADOS E SEUS DESAFIOS REGULATÓRIOS NO BRASIL

Monografia apresentada ao Curso de Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito. Área de concentração: Direito Civil.

Orientador: Prof. Dr. Gustavo César Machado Cabral

FORTALEZA

2021

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

J1d Josino, Clarissa Nogueira.
Dados pessoais, segurança pública e investigação criminal: um panorama da proteção de dados e seus desafios regulatórios no Brasil / Clarissa Nogueira Josino. – 2021.
53 f.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2021.
Orientação: Prof. Dr. Gustavo César Machado Cabral.

1. Dados pessoais. 2. Proteção de dados. 3. LGPD. 4. Segurança pública. 5. Persecução penal. I. Título.
CDD 340

CLARISSA NOGUEIRA JOSINO

DADOS PESSOAIS, SEGURANÇA PÚBLICA E INVESTIGAÇÃO CRIMINAL: UM PANORAMA DA PROTEÇÃO DE DADOS E SEUS DESAFIOS REGULATÓRIOS NO BRASIL

Monografia apresentada ao Curso de Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito. Área de concentração: Direito Civil.

Orientador: Prof. Dr. Gustavo César Machado Cabral

Aprovada em: __/__/____.

BANCA EXAMINADORA

_____
Prof. Dr. Gustavo César Machado Cabral (Orientador)
Universidade Federal do Ceará (UFC)

_____
Mestranda Amária Maxine Cordeiro Soares
Universidade Federal do Ceará (UFC)

_____
Mestranda Ana Luiza Barroso Caracas de Castro
Universidade Federal do Ceará (UFC)

AGRADECIMENTOS

À minha família, meu pai, Josivan, minha mãe, Cássia, minha irmã, Jéssica, e minha irmã de coração, Jaqueline, que sempre me apoiaram incondicionalmente nos estudos e em todas as escolhas que já fiz na vida, por serem meus alicerces e pelo imenso amor dedicado a mim durante esses vinte e quatro anos.

Ao meu orientador Prof. Dr. Gustavo Cabral, por ter aceitado prontamente orientar este trabalho de conclusão de curso, por toda atenção, solicitude e confiança em mim depositada. E à minha banca examinadora, composta pelas mestrandas Amária Maxine e Ana Luiza Barroso, que tanto têm a acrescentar ao tecerem suas críticas a este trabalho de conclusão de curso.

Aos meus professores Wiliam Marques, Fernanda Cláudia, Machidovel Trigueiro, ao coordenador Alex Santiago e ao servidor Nelson Santiago, que me ajudaram tanto, cada um com sua parcela, em minha jornada na Faculdade de Direito.

Aos meus bons amigos de faculdade, Luisa, Giulia, Larissa, Vandressa, Thais, Victor, Liana, Ivina, Antônio, Carlos Mazza, Laryssa e Camila, que me acompanharam nesses quase cinco anos, e à minha amiga Luana, que gentilmente me ajudou em várias situações cotidianas.

E a todos aqueles que porventura não foram diretamente mencionados, mas que de alguma forma me incentivaram e apoiaram ao longo da faculdade de Direito.

RESUMO

O objetivo deste trabalho de conclusão de curso é delinear as peculiaridades sobre o tratamento dispensado aos dados pessoais quando utilizados pela administração pública, tendo em vista a sua utilização na promoção da segurança pública e na persecução penal. Diante do avanço brasileiro em relação ao tema, em especial, por conta da aprovação da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), em agosto de 2018, busca-se, ainda, fazer reflexões sobre como compatibilizar a defesa de bens e objetivos coletivos e institucionais, como por exemplo, a segurança pública, e ao mesmo tempo garantir a inviolabilidade de garantias e direitos fundamentais dos indivíduos. Em razão de a LGPD ter excluído de seu próprio escopo as operações de tratamento de dados pessoais voltadas a fins de segurança pública e investigação e repressão de infrações penais, serão aqui demonstrados os principais aspectos do anteprojeto de lei chamado de "LGPD Penal", com base principiológica semelhante à LGPD, mas que tem especificidades próprias para esse recorte.

Palavras-chave: Dados pessoais. Proteção de dados. LGPD. Segurança pública. Persecução penal. LGPD Penal.

ABSTRACT

The bachelor's thesis main focus is to outline the peculiarities regarding the treatment of personal data when used by public administration, considering its use in promoting public security and criminal prosecution. Given the brazilian progress in relation to the theme, in particular, due to the approval of Law No. 13.709/2018 (General Law for the Protection of Personal Data - LGPD), in August 2018, it is also sought to make reflections on how to make the defense of collective and institutional assets and objectives, such as public security, and at the same time ensure the inviolability of guarantees and fundamental rights of individuals. Dueing to the fact that the LGPD has been excluding from its own scope the operations of processing personal data for the purposes of public security and investigation and repression of criminal offenses, the main aspects of the draft bill called "Criminal LGPD ", based on implicit principles similar to those covered by the LGPD, the draft bill still has specificities for this clipping.

Keywords: Personal data. Data protection. LGPD. Public security. Criminal prosecution. Criminal LGPD.

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
CDC	Código de Defesa do Consumidor
CF	Constituição da República Federativa do Brasil de 1988
CNJ	Conselho Nacional de Justiça
CRFB	Constituição da República Federativa do Brasil de 1988
ETS	European Treaty Series
GDPR	General Data Protection Regulation
LGPD	Lei Geral de Proteção de Dados Pessoais
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
StPO	Strafprozessordnung (Código de Processo Penal da Alemanha)

SUMÁRIO

1. INTRODUÇÃO

Conforme ensina o historiador de tecnologia americano Michael S. Mahoney (2005), não há duplicidade de mundos, como se de um lado estivesse o mundo analógico e real e, de outro, o mundo digital e virtual. Há, na verdade, uma transferência do mundo offline, analógico para o computador e as suas redes[1]. A utilização em larga escala de tecnologias interligadas entre si em redes computacionais traz consigo novas chances, mas traz também novos desafios às sociedades liberais modernas.

Atualmente, ao utilizarmos os dispositivos móveis, deixamos rastros digitais em todo lugar, incluindo os dados de "geolocalização", por vezes considerados sensíveis por proporcionarem um panorama esmiuçado sobre os deslocamentos físicos dos indivíduos, com a possibilidade de inferir hábitos, relacionamentos, preferências e diversas outras deduções[2]. Nesse panorama, talvez possamos dizer que não existe mais mundo off-line. O tratamento inadequado desses dados pessoais pode resultar em situações abusivas e ilegais, com repercussões que violam as garantias individuais.

Boa parte da discussão da proteção de dados tem origem na Alemanha. O ponto de partida dessa discussão se encontra em meados dos anos 70. O governo alemão, em 1973, estava querendo promover um censo, com o levantamento amplo de dados da população, o que resultou em bastante resistência. Argumentava-se, principalmente, que essas informações fariam o estado "saber demais" sobre os cidadãos.

O pano de fundo para essa situação era a experiência com o nacional-socialismo alemão, que tentou institucionalizar um modelo onde o Estado sabia "de tudo", claro, dentro dos limites fáticos ao conhecimento a que esse estado estava submetido e o medo em relação às novas tecnologias de processamento automatizado de dados. Na época, tinha-se a concepção de que o uso dessas tecnologias faria os dados "falarem", ou seja, com o cruzamento de dados neutros obter-se-iam novos conhecimentos.

O caso foi julgado pelo Tribunal Constitucional Alemão em dezembro de 1983, e o argumento central da decisão do tribunal[3] foi que não existem dados neutros, e que todo dado

---

[1] Michael Mahoney, The histories of computing(s): in: Interdisciplinary Science Reviews, 30 (2005), S. 119–135;

[2] PIMENTA, Victor Martins; PIMENTA, Izabella Lacerda; DONEDA, Danilo. Onde Eles estavam na hora do crime? Ilegalidade no tratamento de dados pessoais na monitoração eletrônica. IN Revista Brasileira de Segurança Pública, vol. 13. N. 1, Mar. 2019.

[3] O caso versou sobre diversas reclamações constitucionais ajuizadas por grupos de cidadãos que impugnavam a lei federal de recenseamento alemã, editada em 1982, que havia sido aprovada por unanimidade tanto pelo

obtido é relevante. E ainda, que o cidadão, para que possa se desenvolver numa sociedade livre, deve ter o poder de saber quem, quando e em que ocasião sabe o quê sobre aquele indivíduo. O tribunal postulou, então, derivado de um direito explícito na constituição alemã, qual seja, o livre desenvolvimento da personalidade, um direito à autodeterminação informacional, que é justamente o direito de o cidadão saber o que o estado sabe sobre ele.

Esse direito está afetado a partir do momento em que o estado obtém algum conhecimento sobre o cidadão e quando faz algum uso desse conhecimento. A partir daí, o tribunal deriva uma ideia fundamental nesse setor jurídico, que é a de que a atividade do estado de produção de conhecimento sobre o cidadão e de utilização desse conhecimento é uma intervenção na esfera privada dele.

A proteção de dados pessoais remete ao "conjunto de regras que visam impedir o tratamento inadequado, injusto ou antiético de dados pessoais" (ARTESE, 2017, p. 2). O tema vem ganhando cada vez mais destaque no Brasil, em especial, por conta da aprovação da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), em 14 de agosto de 2018, com período de *vacatio legis* de 24 meses, segundo a Medida Provisória n. 869/2018. A aprovação dessa lei demonstra um avanço brasileiro em relação ao tema ao prever um rol taxativo de hipóteses de tratamento legal de dados pessoais, dentre as quais está o consentimento do titular. Ademais, são previstos diversos direitos dos usuários, princípios de proteção de dados, responsabilidades dos agentes envolvidos no processamento desses dados e sanções em caso de descumprimento de normas.

Contudo, a LGPD não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais. A lei dispõe que, nesses casos, o tratamento de dados pessoais será regido por legislação específica. Nada obstante, não se pode afirmar que

---

Parlamento quanto pelo Conselho Federal. O texto legal previa que no ano de 1983 seria realizado um censo por parte de funcionários públicos e demais agentes encarregados, que não se limitaria apenas a fazer o levantamento do número de habitantes do país, mas também de coletar uma série de outros dados pessoais dos cidadãos. Em sede de liminar, o Tribunal Constitucional Federal suspendeu os efeitos da lei de recenseamento e acabou por julgar parcialmente procedentes as reclamações constitucionais. Em sua base, a realização do censo foi mantida, mas foi consideravelmente modificada, conforme as ordens do Tribunal, para que fosse procedida por meios que resguardassem a segurança dos dados dos cidadãos a serem entrevistados, como por exemplo, pela proibição de que alguns dados obtidos, como nome e endereço, fossem transferidos a outros órgãos de governo. (MENKE, Fabiano. A Proteção de Dados e o Direito Fundamental à Garantia da Confidencialidade e da Integridade dos Sistemas Técnico-Informacionais no Direito Alemão. REVISTA JURÍDICA LUSO-BRASILEIRA, ANO 5, Nº 1. Lisboa, Portugal, 2019 – p. 783/784)

estas aplicações não possam gerar riscos jurídicos, seja pela potencial violação de disposições da Constituição, seja por conflito com normas legais existentes.

Um exemplo ilustrativo é a discussão a respeito do fornecimento, pela empresa Google, de dados de usuários na investigação do assassinato da vereadora Marielle Franco (PSOL-RJ) e seu motorista Anderson Gomes. No caso, cada usuário atingido pela medida seria identificado pelo seu IP, sigla em inglês para protocolo de internet —que funciona como uma impressão digital dos seus respectivos acessos à internet.

A questão controversa é que, segundo a empresa, fornecer esses dados à investigação viola a privacidade de milhões de usuários alheios ao crime para poder chegar aos culpados, o que exigiria, por exemplo, cuidados especiais para garantir a proteção destes dados e evitar o uso destes dados para finalidades inadequadas. Portanto, é interessante e urgente, tanto para o governo quanto para a sociedade civil, a delimitação das condições para o adequado uso dos dados pessoais para segurança pública e investigação criminal.

A relação entre proteção de dados, segurança pública e persecução penal vem ganhando destaque com a apresentação, em novembro de 2020, do "Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal". O anteprojeto, que é chamado de "LGPD Penal", tem o seu motivo, pois, analisando o art. 4º da LGPD, onde constam as situações onde a lei não se aplica, no inciso III:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> [...]
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais;

Dentre as quatro situações descritas no art. 4º, o anteprojeto cobre as questões da segurança pública e da persecução penal, mas não as de defesa nacional e segurança do Estado. Dentro dessa perspectiva, segundo o Ministro Nefi Cordeiro (STJ), elaborar este projeto adveio da necessidade prática da modernização das tecnologias na persecução penal ao redor do mundo[4].

O objetivo é compatibilizar o uso das novas tecnologias pelos órgãos do estado para exercerem suas funções de modo eficiente com as garantias processuais e os direitos fundamentais dos titulares dos dados envolvidos. Visa, ainda, trazer uma complementação da

[4] Webinário Proteção de Dados, segurança pública e persecução penal. [jan. 2021]. Instituto LGPD – Legal Grounds for Privacy Design. Brasil, 2021. Youtube (141 min.)

legislação pátria, a exemplo das lei 12.850/2013 (Lei de Organizações Criminosas), 9.296/1996 (Lei de Interceptações Telefônicas), 12.965/2014 (Marco Civil da Internet), bem como o próprio Código de Processo Civil e outras leis, trazendo um microssistema voltado à proteção de dados na esfera penal e processual penal.

Especialmente nesse debate, há uma tensão inerente, que ocorre em todo e qualquer debate ou proposta legislativa nesse contexto, e a pergunta que decorre dessa tensão é: como compatibilizar a defesa de bens e objetivos coletivos e institucionais, como por exemplo, a segurança pública, e ao mesmo tempo garantir a inviolabilidade de garantias e direitos fundamentais do indivíduo?

Esse é o desafio que iremos debater ao longo deste trabalho de conclusão de curso. O objetivo deste trabalho não é de esgotar o tema, e tampouco trazer uma só resposta correta para os questionamentos que naturalmente surgem, mas sim exibir as peculiaridades e fazer reflexões sobre esse assunto tão atual e tão necessário em nossa sociedade.

2. BASES HISTÓRICAS DA PROTEÇÃO DE DADOS

2.1 Da *Privacy* Americana à Autodeterminação Informacional

Até o final do século XIX, as violações à privacidade dos indivíduos não eram assunto para se resolver perante os tribunais norte-americanos e ingleses. Naquela época, as cortes ocupavam-se em reparar situações de violência ou de ataques à propriedade privada e, em realidade, havia certo receio de que a proteção a interesses intangíveis, como a tutela da esfera íntima, pudesse levar a uma inundação de litígios (MULLER, 1971, p. 169-209).

Por outro lado, num país ainda predominantemente rural, eram relativamente pequeno os danos provocados por violações à privacidade alheia; não havia, ainda, os meios de comunicação de massa – jornais, rádio, televisão e computadores -e o controle social era tão severo quanto fosse a extensão da invasão da privacidade dos indivíduos (por mecanismos morais, não jurídicos). Aliás, a eclosão do *right to privacy* nos Estados Unidos deu-se justamente na substituição de um perfil rural por outro urbano (DONEDA, 2006, p. 265).

A tecnologia gradativamente adentrou na sociedade como divisor de águas neste cenário. As informações, naturalmente, passaram a circular com mais velocidade e abrangência, sem a possibilidade de comprovação de sua veracidade por conhecimento direto da situação noticiada. As repercussões trazidas por esta nova formatação social redundaram no primeiro texto que reclamou proteção jurídica à esfera privada.

A origem da proteção à privacidade na Common Law não adveio de um caso em específico, mas num artigo publicado por dois juristas, Samuel D. Warren e Louis D. Brandeis (1890), na *Harvard Law Review*, intitulado *The right of privacy*[5]. O texto, que inicia afirmando que do direito à vida logo se passou ao direito de aproveitar a vida (*right to enjoy life*), ou *the right to be let alone* (o direito de ser deixado em paz), ressalta que o direito à propriedade ampliou seu alcance para a ideia de propriedade intangível (autoria de obras de arte, segredos comerciais, por exemplo).

Os juristas autores da obra, contudo, logo demonstram a preocupação – ainda atual à realidade de nosso século – de que o maldizer não era mais o recurso do ocioso e dos perversos, mas tinha-se tornado um negócio, perseguido com ousadia por alguns. Assim

[5] BRANDEIS, Louis D.; WARREN, Samuel D. The right of privacy. Harvard Law Review, Boston, v. IV, n. 5, dec. 1980. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: mar. 2021.

sendo, o propósito do artigo foi o de verificar se o direito vigente na Common Law preceituava um princípio que pudesse ser invocado para proteger o direito à privacidade e, em caso afirmativo, qual o alcance dessa proteção[6].

A partir deste ponto inicial, desenvolveu-se o pensamento de que o indivíduo teria o direito de decidir sobre a publicização de informações privadas do qual é titular. Daqui tem-se a matriz[7] do que o Tribunal Constitucional Federal alemão, anos depois, em 1983, definiu como o direito à autodeterminação informativa.

Não obstante, antes mesmo da referência expressa à autodeterminação informativa (ou informacional) no sistema jurídico alemão, o Tribunal Constitucional já abordava o assunto de diversas formas, de modo que não houve propriamente a criação do direito em um *case* específico; houve, na realidade, o reconhecimento do status de direito fundamental a uma temática que já contava com certa elaboração jurídica (BUCHNER, 2006, p. 41). É o que se infere da análise de precedentes anteriores à decisão da lei do Censo (*Volkszählungsurteil*[8]), a ser analisada a seguir, na medida em que fazem referência a um direito à autodeterminação do indivíduo sobre seus dados pessoais.

Em 1969, por exemplo, na Mikrozensus-Entscheidung (BUCHNER, 2006, p. 41), foi garantida a autodeterminação aos indivíduos no sentido de poder controlar e fiscalizar o tratamento de seus dados pessoais e as informações relativas à sua vida privada. Destaca-se a ideia de que, para garantir o livre e responsável desenvolvimento de sua personalidade, todo cidadão precisaria permanecer em uma espécie de "espaço interno", no qual ele domina e controla a si próprio e de onde possa se retirar sem sofrer influências externas. Esse espaço deveria permitir que se ficasse em paz e que se aproveitasse um direito de estar só.[9]

---

[6] RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O direito à proteção de dados pessoais e a privacidade. Revista da Faculdade de Direito UFPR, v. 53, 2011.

[7] No entanto, em que pese seja do ordenamento jurídico americano o mérito de iniciar tais debates, em termos de *privacy* como um direito geral de personalidade, há de se ressaltar a problemática opção do senado estadunidense em não adotar um sistema de proteção de dados independente, o que refletiu principalmente nas questões de âmbito privado. Tal déficit de tutela foi levado em consideração pela União Europeia, que tratou do assunto em diferentes convenções e diretivas, estabelecendo o dever te proteção dos dados pessoais em instituições públicas e também em organizações privadas (SCHAAR.Das Ende der Privatsphäre: der Weg in die Uberwachungsgesellschaft. 2007, p. 19-21)

[8] Veredito do censo (tradução nossa).

[9] Assim dispôs a Corte em seu precedente: "[...] Ein solches Eindringen in den Persönlichkeitsbereich durch eine umfassende Einsichtnahme in die persönlichen Verhältnisse seiner Burger ist dem Staat auch deshalb versagt, weil dem Einzelnen um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein "Innenraum" verbleiben muß, in dem er "sich selbst besitzt" und "in den er sich zuruckziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt" [...]."

Em decisões posteriores, a autodeterminação informativa no tocante ao direito geral de personalidade ganhou cada vez mais espaço, e o Tribunal Constitucional Alemão dispôs desta figura jurídica de diversas maneiras. Em grande parte dos casos, era suscitada no sentido de que o indivíduo poderia escolher como ser representado ou visto por terceiros ou pelo público como um todo. A autodeterminação informativa, nesse sentido, abrangeria o direito à própria imagem e àquilo que é dito sobre ele, assim como a possibilidade de dispor sobre a representação de si mesmo (BUCHNER, 2006, p.42).

Em 1977, o ordenamento jurídico Alemão já dispunha de uma lei federal sobre a matéria – notadamente, a primeira do mundo a tratar da proteção de dados pessoais, originária da *Land de Hesse* –, mas que revelou-se incapaz de fornecer garantias suficientes aos cidadãos e de enfrentar a Lei do Censo.

Invocando esta lei, o estado pretendia realizar um censo geral no ano de 1983, que objetivava, a partir de 160 perguntas, comparar os dados fornecidos com os do registro civil. Para mais, as perguntas eram de cunho pessoal, que iam desde as aspirações profissionais do indivíduo até suas práticas religiosas e políticas. Outros pontos que suscitaram controvérsia foram, dentre outros, a possibilidade de transmissão dos dados colhidos a autoridades federais e a outros Länder (como são chamados os estados federados em alemão), a previsão de multa aos que se recusassem a responder ao Censo e a inserção de mecanismos que favorecessem a denúncia desses indivíduos (DONEDA, 2006, p. 192, apud RUARO, 2011, p. 55).

Nesse cenário, proliferou o sentimento de insegurança e o temor da criação de um Estado superinformado, iniciando-se um processo que culminou com a sentença da Corte Constitucional, suspendendo provisoriamente o censo e, após, julgando-o inconstitucional, sob a alegação principal de que, caso os dados recolhidos fossem utilizados ao mesmo tempo para fins administrativos e estatísticos, estaria caracterizada a diversidade de finalidades, o que impediria o cidadão de saber efetivamente sobre o uso de suas informações. Salientou ainda, a Corte, que o rigor estatístico não poderia coexistir com a necessidade dos órgãos administrativos de identificar os titulares de dados.

Tal acontecimento é considerado o marco inicial da autodeterminação informativa, que, segundo a sentença, consistiria nos direitos de os indivíduos decidirem por si próprios quando e dentro de quais limites seus dados pessoais poderão ser utilizados. Partindo dessa ideia, o sujeito passa decidir quando e sob que circunstâncias serão do conhecimento alheio os seus dados pessoais. Ressalte-se que o norte-americano Alan Westin, já em 1967,

mencionava essa figura jurídica. Entretanto, ainda que não desenvolvida originariamente pela própria Corte Constitucional, a Sentença da Lei do Censo é apontada pela grande maioria da doutrina como um marco oficial na proteção de dados pessoais (1967, p. 7)[10].

Especificamente no direito alemão, esse julgado é considerado a Constituição da proteção de dados pessoais, na medida em que a decisão trouxe suporte para a discussão constitucional sobre a intervenção e controle Estatal neste âmbito. Desde então, passou-se a exigir que cada limitação ou restrição ao direito à autodeterminação informativa tivesse respaldo constitucional[11].

Buchner (2006, p. 46), conforme citado por Ruaro (2011, p. 56) explica a necessidade de clareza na atuação do Poder Público ao restringir o direito, assim como a necessidade de congruência entre o motivo legal e a efetiva coleta de dados. Dessa forma, a proteção dos dados pessoais é a regra, e a intervenção estatal, a exceção. O ente estatal deve sempre, ao tratar estes dados, atuar em consonância com as disposições legais, respeitando, dentre outros princípios, a proporcionalidade.

2.2 Inviolabilidade de dados pessoais e direito à privacidade no ordenamento jurídico brasileiro

Ao se falar em proteção de dados pessoais, necessariamente se fala no direito fundamental à privacidade, eis que aquela pode ser compreendida como espécie desse gênero. Ambos estão positivados em nossa Constituição Federal de 1988, no art. 5º, incisos X e XII, que assim dispõem:

> "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"
>
> "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual pena"

Nas palavras de Tércio Sampaio Ferraz Júnior (1993, p. 452), "Em questão está o direito de o indivíduo excluir do conhecimento de terceiros aquilo que a ele só é pertinente e que diz respeito ao seu modo de ser exclusivo no âmbito de sua vida privada."

A privacidade constitui direito subjetivo fundamental. Enquanto direito subjetivo, tem como base três elementos, a saber, sujeito, conteúdo e objeto. Conforme Ferraz Júnior

[10] WESTIN, Alan. (1967). Privacy and Freedom. New York, Atheneum, apud RUARO (2011, p. 56)
[11] RUARO, Regina Linden (2011, p. 56)

(1993, p. 440) o sujeito é o titular do direito. Consagrado na Constituição Federal, o sujeito é toda e qualquer pessoa, física ou jurídica, brasileira ou estrangeira, residente no País (CF, art. 5º, *caput*).

O conteúdo, segundo o autor, corresponde à prerrogativa específica atribuída a um sujeito, que pode ser a de constranger os outros, de resistir-lhes ou de dispor, gozar e usufruir. Enquanto direito, a privacidade tem por conteúdo a prerrogativa de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por dizerem a ele só respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão.[12]

O objeto, por sua vez, consiste no bem juridicamente protegido, que pode constituir-se uma coisa - não necessariamente física, em se tratando de direitos reais - ou um interesse (na hipótese de direitos pessoais). No direito à privacidade, de forma sintética, o objeto é a integridade moral do sujeito. A Declaração Universal dos Direitos Humanos, de 1948, traz em seu art. 12 os elementos conteúdo e objeto de forma elucidativa: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda pessoa tem direito à proteção da lei".

No Brasil, uma ideia embrionária de proteção à privacidade surge com a Constituição de 1891, em seu art. 72, §18, que dispunha ser inviolável o sigilo das correspondências. No mesmo sentido, seguiram-se as Constituições brasileiras de 1934 (artigo 113, §8º) e de 1946 (artigo 141, §6º).

Ainda que tardiamente, a Constituição brasileira de 1967 ampliou, em seu artigo 150, § 9º, o que até então se entendia como proteção à privacidade, passando a proteger o sigilo das comunicações telegráficas e telefônicas, e não apenas a inviolabilidade das correspondências. Isso pois as constituições brasileiras restringiam a "privacidade" a uma proteção às comunicações, carecendo de dispositivos que efetivamente protegessem a vida privada do cidadão de interferências externas.

Contudo, somente com a Constituição Federal de 1988 é que houve uma efetiva majoração da importância do direito à privacidade, de tal sorte que conceitos antes muito

[12] FERRAZ JÚNIOR, 1993, p. 440.

limitados (privacidade) ou mesmo inexistentes (intimidade) passaram a figurar como direitos e garantias fundamentais dos cidadãos[13].

A inviolabilidade do sigilo de dados, por seu turno, remete ao "conjunto de regras que visam impedir o tratamento inadequado, injusto ou antiético de dados pessoais" (ARTESE, 2017, p. 2). Como já dito alhures, a proteção de dados pessoais é uma dimensão da privacidade, direito de personalidade assegurado pela nossa Constituição da República em seu art. 5º, além dos arts. 11 e 21[14] do Código Civil (Brasil, 2002), dentre outros dispositivos, como o art. 1º, III da CRFB/88, que assegura o direito à dignidade da pessoa humana.

Outros normativos constitucionais e legislativos asseguram essa proteção. O *habeas data*, por exemplo, previsto no art. 5º, LXXII da CF/88, representa o direito personalíssimo do titular de controlar as informações/dados pessoais, constantes em registros públicos ou privados, e a manter, alterar, explicar e excluir essas informações.[15] Ele abrange, assim, o direito de acesso, de retificação e de complementação em relação aos dados pessoais. Ressalte-se que com a instituição desse remédio constitucional, o Brasil foi o primeiro país a conceber garantia própria para a proteção de dados. Após, outros países introduziram em suas legislações tais previsões de formas variadas.

O primeiro diploma legal brasileiro a fazer menção ao termo "dados pessoais" foi o de nº 8.078/1990, o chamado Código de Defesa do Consumidor, em seu art. 43. Há uma importante correlação entre a proteção do consumidor e a de dados pessoais. Isso pois o tratamento de dados, capaz de ensejar violações à privacidade, por muitas vezes acontece entre empresas, prestadores de serviços de conteúdo e de conexão e outros agentes considerados fornecedores, nos termos do art. 3º do CDC, assim como aquelas pessoas que podem ser enquadradas como consumidoras, conforme o art. 2º do mesmo diploma (SILVA, 2019, p. 9).

A Lei 12.527/2011, também chamada Lei de Acesso à Informação, estabelece em seu artigo 4º, IV, que informação pessoal é "aquela relacionada à pessoa natural identificada ou identificável" e visa aumentar a transparência por parte da administração pública direta e

---

[13] BARBOSA; DA SILVA; 2019, p. 491.

[14] Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.
Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

[15] Nesse sentido, NIESS, 1990; ROTHEMBURG, 1998; UICICH, 1999; MORAES, 2009; FERRAZ, 2008; SILVA, 2009, 2012; MOURÃO NETO, 2012.

indireta, nos três Poderes e em todas as esferas governamentais, ao disponibilizar a qualquer pessoa, seja ela física ou jurídica, informações de caráter público sem exigir nenhuma motivação para o pedido.

A principal diretriz dessa lei, em consonância com a Constituição Federal, é que "a publicidade e a transparência das informações são a regra e o sigilo é a exceção". Ou seja, qualquer dado sob a guarda do Estado deve, de regra, ser público.

O Marco Civil da Internet, por sua vez, em seu art. 3º, III, traz a proteção de dados pessoais como um dos seus princípios fundantes.

Segundo Doneda (2011, p. 94), existe uma diferença entre os conceitos de informação e dado: "Dado é conceituado como a representação bruta de um fenômeno, sem elaboração, ao passo que informação é o dado trabalhado, interpretado". Apesar disso, diante da ausência de uma definição objetiva até então, passou-se a utilizar uma interpretação analógica do conceito de dado pessoal com o de informação pessoal.

Uma definição objetiva de dado pessoal surgiu somente em 2018, com a sanção da Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), em seu art. 5º, inciso I, como sendo uma "informação relacionada a pessoa natural identificada ou identificável".

Com recentíssima entrada em vigor, a LGPD inova ao trazer para o ordenamento jurídico pátrio questões não satisfatoriamente tratadas por outras leis setoriais de proteção de dados existentes no Brasil. No item seguinte, detalharemos as principais inovações trazidas pela LGPD.

2.3. A Lei Geral de Proteção de Dados

Contextualizando brevemente o cenário das leis de proteção de dados a nível mundial, a primeira lei específica nesse sentido surgiu na Europa em, 1970, no estado alemão de Hesse[16]. Em seguida, várias leis similares despontaram ao redor do mundo, como na Suécia em 1973, e Dinamarca e França em 1978, tendo em vista a crescente preocupação em proteger os dados pessoais dos cidadãos não apenas do governo, mas também das empresas privadas (BARBOSA; DA SILVA; 2019, p. 498).

Somente em 2005 o Brasil foi provocado pela Argentina, que já contava com uma lei geral de proteção de dados desde 1994, a instituir normativo similar, haja vista o Brasil fazer parte do Mercosul e levando em conta a necessidade de uniformizar a legislação sobre o tema

[16] FREUDE, Alvar; FREUDE, Trixy. Echoes of History: Understanding German DataProtection. 2016. Disponível em: <https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/>. Acesso em: 15 mar. 2021.

entre os países-membros, assim como de harmonizá-las com a legislação de países parceiros nas relações econômicas. Nesse sentido, ensina o desembargador Demócrito Reinaldo Filho[17]:

> "O Brasil vinha perdendo oportunidades de investimento financeiro internacional em razão do "isolamento jurídico" por não dispor de uma lei geral de proteção de dados pessoais. A União Europeia, por exemplo, veda a transferência de dados de cidadãos europeus para empresas de outros países que não têm um "nível adequado" de proteção de dados pessoais, e o Brasil até então era enquadrado na categoria das nações que não protege de maneira satisfatória a privacidade e intimidade das pessoas."

Até muito recentemente, as ferramentas disponíveis na legislação pátria ofereciam uma proteção genérica para os dados pessoais, que, devido à complexidade das técnicas de coleta e processamento de dados, mostrava-se pouco precisa e não oferecia garantias adequadas às partes.

Somente no ano de 2018 houve a sanção da Lei 13.709/2018, a chamada Lei Geral de Proteção de Dados, alguns meses após a entrada em vigor da General Data Protection Regulation – mais conhecida como GDPR, que consiste em uma reforma legislativa aplicada à União Europeia e ao Espaço Econômico Europeu com o objetivo de regular a proteção da privacidade e dos dados pessoais.

Em razão do poderio econômico da União Europeia, qualquer país que desejasse permanecer estabelecendo relações econômicas ou de qualquer outra natureza que envolvesse troca de dados e informações com os países da UE, necessariamente deveria se adequar às diretrizes impostas. Assim, ante à globalização comercial, ao elevado fluxo de tratamento de dados e às relações de vários países do mundo com a Europa, houve uma tendência global de adequação à GDPR[18].

A nação que, porventura, não se adequasse, teria prejudicada sua relação com os países-membros da União Europeia. Com isso, diversos países, incluindo o Brasil, trataram de, rapidamente, criar aparatos legais que atendessem aos padrões de transparência sobre o uso e tratamento dos dados pessoais adotados pela União Europeia. Dessa forma, a Lei Geral de Proteção de Dados do Brasil é também uma reação do país às exigências do mercado globalizado[19].

Não obstante a vigência da GDPR tenha porventura pressionado, ainda que indiretamente, a sanção da Lei 13.709/2018 no Brasil, uma análise do contexto histórico revela

---

[17] REINALDO FILHO, Demócrito. Lei de proteção de dados pessoais aproxima o Brasil dos países civilizados. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 23, n. 5498, 21 jul. 2018. Disponível em: <https://jus.com.br/artigos/67668>. Acesso em: 15 mar. 2021.

[18] BARBOSA; DA SILVA; 2019, p. 499

[19] Ibidem

que o país, há muito, carecia de regulamentação específica que devolvesse aos cidadão a autonomia sobre seus próprios dados pessoais e criasse um ambiente seguro para a circulação desses dados, com vistas ao respeito da privacidade, pautada nos direitos humanos e ensejando o livre desenvolvimento da personalidade, dignidade e o exercício da cidadania pelas pessoas naturais.

Com a publicação da LGPD, os direitos dos usuários (como o da confirmação da existência de tratamento; acesso; correção de dados completos, inexatos ou desatualizados; anonimização e eliminação de dados desnecessários; portabilidade dos dados a outro fornecedor e revogação do consentimento, previstos no art. 18 da Lei n. 13.709/2018), em conjunto com os princípios da proteção de dados pessoais, vieram com o objetivo de trazer limites claros no âmbito do tratamento desses dados no Brasil. Para Somadossi (2018)[20]:

> "A LGPD cria uma regulamentação para o uso, proteção e transferência de dados pessoais no Brasil, nos âmbitos privado e público, e estabelece de modo claro quem são as figuras envolvidas e quais são suas atribuições, responsabilidades e penalidades no âmbito civil – que podem chegar a multa de 50 milhões de reais por incidente."

Tal delimitação, per si, é um ponto bastante positivo da Lei Geral de Proteção de Dados, vez que determina de especial e objetivamente os agentes, suas responsabilidades, o que devem ou não fazer e como fazer, de maneira a facilitar a aplicabilidade da norma de maneira homogênea, o que, até então, não era possível concretizar apenas com os dispositivos legais genéricos que se dispunha.

O limite de alcance da LGPD está disposto em seu art. 3º, que estabelece que qualquer operação de tratamento de dados está sujeita a ela. Entretanto, é necessário que tal operação, seja ela realizada por pessoa jurídica ou natural, decorra de dados que tenham sido tratados ou coletados no Brasil, e que o tratamento desses dados tenha como finalidade a oferta de bens ou serviços ou que os titulares desses dados estejam situados no Brasil.

No art. 4º, a LGPD resolve sobre as causas excludentes de sua aplicabilidade, quais sejam: o tratamento de dados realizado por pessoas naturais apenas para fins particulares e não econômicos e o tratamento de dados com fins exclusivamente jornalísticos, artísticos ou acadêmicos. Outras hipóteses que estão fora do escopo de proteção da lei, estas previstas no inciso III, ocorrem quando o tratamento de dados pessoais são utilizados pela Administração

[20] SOMADOSSI, Henrique. O que muda com a Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.migalhas.com.br/dePeso/16,MI286235,31047/O+que+muda+com+a+Lei+Geral+de+Protecao+de+Dados+LGPD.

Pública para fins exclusivos de defesa nacional, segurança pública ou atividades de investigação ou repressão de infrações penais. O parágrafo 1º do art. 4º dispõe que:

> "[...] o tratamento será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei."

Uma última hipótese de exclusão da aplicabilidade da LGPD diz respeito a dados provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na Lei.

No quinto artigo, o normativo pontua algumas definições relevantes, algumas já abordadas alhures, a exemplo da definição de dados pessoais. No entanto, esse artigo também traz à baila alguns outros conceitos importantes para o estudo do tema, como é o caso do dado pessoal sensível (Artigo 5º, inciso II da LGPD):

> "[...] dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural."

É de se notar que os dados considerados sensíveis estão destacados dos dados pessoais gerais. Esse destaque é pertinente justamente por se tratarem de informações que podem acarretar discriminações, caso se tornem públicas. Diante disso, eles gozam de uma proteção específica na Lei: o art. 11 autoriza o tratamento de dados sensíveis apenas quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; para cumprimento de obrigação legal do controlador; com o fim de realização de estudos por órgão de pesquisa, entre outras hipóteses (BRASIL, 2018).

Outra definição interessante trazida pelo art. 5º é o consentimento. Pode-se dizer que a autodeterminação informacional tem repercussões ainda nos dias atuais, já que uma das hipóteses de legitimidade do tratamento legítimo de dados tanto na legislação europeia, quanto na brasileira, continua a ser o consentimento[21].

Sobre o tema, Laura Mendes (2014, p. 57) ensina que o consentimento é um instituto jurídico para "fazer valer a autonomia privada do cidadão", considerando os componentes autoconformação e liberdade do titular na proteção de dados pessoais. Mendes afirma, ainda, que o consentimento tem natureza atípica para o processamento de dados, visto que ele apresenta características negociais e, ao mesmo tempo, possui caráter

[21] SILVA, 2019, p. 804.

personalíssimo, sendo possível aplicar as regras relativas aos negócios jurídicos e contratos ao consentimento, sempre que se mostrar adequado (MENDES, 2014, p. 60).

A LGPD dispõe que o consentimento deverá ser "uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (Art. 5º, XII da Lei n. 13.709/2018). Contudo, o consentimento como ferramenta de controle dos indivíduos sobre suas informações possui forma de implementação complexa, em um contexto de constante inovação tecnológica, já que nem sempre a pessoa consegue dimensionar as consequências de uma disposição de seus dados (MENDES, 2014, p. 58-59).

Nessa toada, Daniel J. Solove afirma que, apesar do modelo da autodeterminação informativa ou, como o autor nomeia, "*privacy self-management*" ser um componente necessário de qualquer regime regulatório, ele está sendo usado para além de suas capacidades, vez que existem problemas cognitivos e estruturais que prejudicam a capacidade do indivíduo de autogerir sua privacidade (SOLOVE, 2013, p. 1.880).

O artigo sexto e incisos da LGPD dispõem sobre os princípios que regem o tratamento de dados pessoais, a saber, a finalidade, que assegura que o tratamento de dados somente poderá ocorrer para a finalidade que ensejou a coleta dos dados pessoais, ou seja, não será possível tratar tais dados para outros fins após ter sido atingido o objetivo principal do tratamento. Desse modo, os dados pessoais não poderão ser utilizados irrestritamente; a adequação, que dispõe que os dados pessoais coletados têm que ter um tratamento limitado à finalidade almejada, coibindo, portanto, arbitrariedades nesse tratamento; a necessidade, que ordena que deve se reduzir ao mínimo o tratamento de dados pessoais para se alcançar uma finalidade; o livre acesso, que garante ao titular do dado pessoal o acesso livre e facilitado aos seus próprios dados; a qualidade, que é uma garantia aos titulares de que seus dados são exatos, claros e estejam atualizados para a finalidade objetivada pelo tratamento; a transparência, que dispõe que nenhum dado pode ser tratado sem que seus titulares conheçam o objetivo desse tratamento; a segurança, que trata da necessidade de adoção de medidas para proteger os dados pessoais de ataques externos que visem sua destruição, perda, alteração, comunicação ou difusão; a prevenção, que corresponde a medidas de caráter preventivo que evitem a ocorrência de danos em virtude do tratamento de dados pessoais; a não discriminação, que consiste em evitar que o tratamento de dados pessoais objetive discriminar seus titulares e, por fim, a responsabilização e prestação de contas, que objetivam garantir que os agentes que tratam os dados pessoais busquem soluções que lhes permitam obedecer aos princípios anteriores da melhor forma possível.

Outro aspecto relevante da LGPD diz respeito aos limites que o controlador dos dados pessoais, ou seja, aquele toma as decisões em uma empresa para definir como os dados serão tratados, pode exercer (art. 10), apresentando um rol de situações concretas que permitem o controlador tratar dados pessoais com finalidades permitidas em lei.

Já o artigo 18 da LGPD dispõe sobre os direitos que o titular de dados pessoais tem perante aqueles que tratam seus dados, sendo eles: a) direito à confirmação: saber se os dados estão ou não sendo tratados; b) acesso: acessar seus dados a qualquer tempo; c) retificação: pode o titular retificar seus dados caso detecte alguma inexatidão ou estejam desatualizados; d) anonimização: bloquear ou eliminar dados desnecessários ou em excesso para a finalidade que se deseja obter como resultado do tratamento; e) portabilidade: o titular pode portar seus dados de um serviço ou produto para outro de natureza concorrente; f) eliminação de dados: pode o titular requerer o apagamento de seus dados pessoais tratados, com algumas ressalvas; g) informação: o titular tem o direito de ser informado por entidades públicas ou privadas se seus dados foram compartilhados; h) revogação do consentimento: em que o titular pode cessar o consentimento sobre o tratamento dos seus dados.

Há, ainda, regras que concedem ao Estado permissão para o tratamento de dados pessoais com o objetivo de satisfazer o interesse público. Essas regras determinam diretrizes para a transferência internacional de dados pessoais em um rol taxativo, e também estabelecem situações em que os tratadores dos dados pessoais poderão ser responsabilizados, acaso causem danos de ordem patrimonial, moral, individual ou coletivo aos indivíduos em violação à legislação de proteção de dados pessoais, devendo reparar tais danos.

Entretanto, talvez a maior inovação trazida pela Lei Geral de Proteção de Dados em relação à tutela dos dados pessoais seja a criação de meios mais eficazes para evitar que ocorram violações aos direitos dos titulares.

A Lei traz um capítulo destinado às sanções administrativas aplicadas aos agentes de tratamentos de dados que violarem seus dispositivos, inclusive estipulando a aplicação de multas que podem chegar a R$50.000.000,00 (cinquenta milhões de reais).

Muitas das disposições contidas na lei, entretanto, dependem de regulamentação de um órgão, cujo objetivo é ser um "guardião" da LGPD e do direito à privacidade: a Autoridade Nacional de Proteção de Dados (ANPD).

A lei que alterou a LGPD para a criação da ANPD (Lei Federal 13.853/19) foi publicada em 9 de julho de 2019. Com a inclusão do art. 55-A na lei protetiva de dados, estabeleceu-se que o órgão faria parte da administração pública federal, sendo integrante da Presidência da República.

Sobre a lei 13.853/19, cumpre destacar que esta definiu como transitória a natureza jurídica da ANPD, e, além disso, determinou a estrutura do conselho diretor do órgão, dispôs sobre os cargos em comissão, bem como estabeleceu as 24 (vinte e quatro) competências da Autoridade. A ANPD deverá não apenas zelar e ser guardião da privacidade e da proteção de dados pessoais, como também atuar ativamente na regulamentação e fiscalização relativas à lei.

Note-se, à vista do que ocorreu até o momento, que se espera uma postura muito mais atuante do que a que apresenta a Autoridade de Proteção de Dados. Sua estruturação tardia gera receios em diversos setores, mormente considerando que a LGPD foi aprovada em meados de 2018, tendo havido, na opinião de alguns, prazo suficiente para a regulamentação de questões essenciais[22].

Outro aspecto que está sendo objeto de discussão é se, na prática, a ANPD terá a autonomia necessária que este tipo de órgão exige, a exemplo das autoridades internacionais. O Conselho Diretor traz em sua maioria militares, o que não se assemelha a nenhuma outra autoridade de proteção de dados em países referências sobre o tema.

É pertinente destacar, ainda, que a participação da ANPD em qualquer questão que, direta ou indiretamente, se relacione com proteção de dados, deve ser incisiva e objetiva. Recentemente, um vazamento de mais de 220 milhões de CPFs colocou especialistas e titulares de dados em alerta. Na oportunidade, esperava-se um posicionamento imperioso da ANPD, mas o que aconteceu – e causou decepção - foi a ausência de qualquer manifestação pública da Autoridade diante da grandiosidade da extensão de danos que esse tipo de incidente pode causar à sociedade civil brasileira.

Enquanto todos os componentes envolvidos na prática e aplicação da LGPD aguardam ansiosamente atuações mais imponentes da Autoridade Nacional de Proteção de Dados, deve-se ter em mente que, além de a Autoridade ter sido instituída tardiamente, pressionada e sem recursos, há diversos itens de complexa regulamentação na LGPD e um panorama extremamente desafiador para a proteção de dados no país. Talvez não fosse razoável esperar que ANPD estivesse apta a investigar casos complexos de vazamento de dados pessoais com tão poucos "meses de vida"[23].

---

[22] GUEIROS, Paula M.; MACIEL, A.C.T. A atuação da Autoridade Nacional de Proteção de Dados (ANPD). Migalhas. Brasil, 2021. Disponivel em: <https://www.migalhas.com.br/depeso/341872/a-atuacao-da-autoridade-nacional-de-protecao-de-dados-anpd >

[23] GUALDA, Diego. A responsabilidade da ANPD e os recentes casos de vazamentos de dados. Site Estadão. Disponível em: < https://politica.estadao.com.br/blogs/fausto-macedo/a-responsabilidade-da-anpd-e-os-recentes-casos-de-vazamentos-de-dados/>

Dito isso, a cobrança sobre a ANPD nos últimos casos sobre vazamento de dados deve ser realizada dentro de um contexto mais amplo. Entretanto, é essencial que tenhamos um poder de julgamento apurado sobre a questão, pois a atuação dos diretores e demais agentes que compõem a Autoridade devem acompanhar a tendência de atuação das grandes referências mundiais em proteção de dados para fins de sedimentar o caminho da LGPD da forma mais satisfatória possível.

3 PROTEÇÃO DE DADOS, SEGURANÇA PÚBLICA E PERSECUÇÃO PENAL - O QUE A LGPD DEIXOU DE FORA?

Na medida em que a sociedade moderna torna-se cada vez mais mediada por aparelhos e tecnologias do mundo digital, o direito carece necessariamente da adaptação de seus institutos às novas condições da sociedade. Com a entrada em vigor da Lei nº 13.709/2018 (LGPD- Lei Geral de Proteção de Dados Pessoais), a extensão desse debate para a investigação e processo penal denota justamente a inevitabilidade da reflexão jurídica em torno da criação de novos mecanismos de proteção de direitos fundamentais[24].

O grande desafio em torno da matéria é conciliar, de um lado, a necessária segurança jurídica para as autoridades se utilizarem de dados pessoais no âmbito de suas atividades, e, de outro lado, garantir ao cidadão que seus dados pessoais não serão usados de modo abusivo, equivocado ou discriminatório pelas autoridades[25].

De acordo com Danilo Doneda e Laura Mendes (2018, p. 469), é possível "identificar cinco eixos principais da Lei Geral de Proteção de Dados em torno dos quais a proteção do titular de dados se articula: i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados; v) responsabilização dos agentes".

É possível visualizar, a partir desse rol, que, em princípio, a Lei Geral de Proteção de Dados seria aplicável à jurisdição penal no que diz respeito à unidade e generalidade de sua aplicação, ou seja, a Lei Geral de Proteção de Dados possui características de uma Lei Geral[26].

Essa aplicabilidade potencial, entretanto, não é concretizada quando da análise do artigo 4º, III, que exclui de seu próprio escopo as operações de tratamento de dados pessoais

---

[24] Instituto LGPD - Legal Grounds for Privacy Design. Site do instituto. Observatório Nacional de Regulação Digital. Disponível em: <https://institutolgpd.com/observatorio_nacional/>

[25] *Ibidem*

[26] Sobre o tema, Doneda: "O primeiro eixo diz respeito ao âmbito de aplicação material da Lei, caracterizado pela generalidade e unidade: a Lei concentra-se na proteção dos dados do cidadão, independentemente de quem realiza o seu tratamento, aplicando-se, assim, tanto aos setores privado e público, sem distinção da modalidade de tratamento de dados (art. 3o). O seu âmbito de aplicação abrange também o tratamento de dados realizado na Internet, seja por sua concepção de Lei geral, seja por disposição expressa de seu art. 1o. Essas são características fundamentais em uma Lei geral, que permitem a segurança do cidadão quanto aos seus direitos independentemente da modalidade de tratamento de dados e quem o realize, bem como proporciona isonomia entre os diversos entes que tratam dados, o que facilita o seu fluxo e utilização legítimos".
(MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor. 2018. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1116.

voltadas a fins de segurança pública, defesa nacional, segurança do Estado ou investigação e repressão de infrações penais.

Um dos grandes problemas da norma começa quando, além do art. 4º, o intérprete passa a analisar o art. 33, III, que dispõe que a transferência internacional de dados pessoais somente é permitida quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional.

Ou seja, ao passo que a lei não é aplicável no âmbito das investigações criminais nacionais, discorre sobre eventual cooperação internacional entre autoridades alienígenas com a brasileira.

A partir do presente estudo, o questionamento que surge é se, ao dispor sobre a matéria dessa forma, teria a Lei Geral de Proteção de Dados agido corretamente, ou se foi perdida uma importante oportunidade de regulamentação do tema.

3.1. Dados de geolocalização e a investigação do caso Marielle Franco

A jurisprudência brasileira, representada pelos Tribunais Superiores, tem se debruçado sobre o acesso a dados e uso da tecnologia como instrumento de efetivação da tutela jurisdicional penal[27].

A análise de dados (*data analytics*) se mostra eficaz em múltiplas atividades relacionados a investigações criminais, como a identificação do local dos crimes e dos criminosos, o monitoramento de suspeitos ou padrões de comportamento criminoso, e com efetividade em casos de pessoas desaparecidas ou sequestradas[28], de forma que a tecnologia deve ser usada para elevar a eficiência e acurácia das investigações. Contudo, a circulação de dados pessoais entre as autoridades competentes para tais efeitos, incluindo a manutenção da segurança pública, deve respeitar as liberdades individuais.

---

[27] Exemplificativamente, na seara do direito penal, no Informativo nº 583, o STJ definiu que "sem prévia autorização judicial, são nulas as provas obtidas pela polícia por meio da extração de dados e de conversas registradas no whatsapp presentes no celular do suposto autor de fato delituoso, ainda que o aparelho tenha sido apreendido no momento da prisão em flagrante. STJ. 6ª Turma. RHC 51.531-RO, Rel. Min. Nefi Cordeiro, julgado em 19/4/2016 (Informativo nº 583 do STJ). Disponível em:<https://www.dizerodireito.com.br/2018/02/acesso-as-conversas-do-whatsapp-pela.html>. Acesso em: 15 mar. 2021.

[28] BRUNTY, Joshua; HELENEK, Katherine. Social Media Investigation for Law Enforcement. Londres/ Nova York: Routledge, 2013, p.57.

Existem, atualmente, vozes utilitaristas no direito penal, que remetem ao ideal iluminista de Beccaria[29] (*apud* Freitas, 2001, p. 76) do século XVIII e não têm obstáculos até mesmo ante à concretização tecnológica do panóptico de Bentham. Contudo, a disponibilidade da tecnologia não autoriza seu uso indiscriminado pelo Estado, sem antes passar pelo crivo dos direitos fundamentais.

Essa questão foi enfrentada em agosto de 2020, pela 3ª Seção do Superior Tribunal de Justiça, que decidiu sobre a quebra de sigilo telemático de dispositivos determinados por geolocalização, para contribuir na investigação do caso da vereadora carioca Marielle Franco e de seu motorista, Anderson Gomes, assassinados em março de 2018, no Rio de Janeiro.

A empresa Google questionou decisão da 4ª Vara Criminal da Comarca do Rio de Janeiro que lhe determinou, em fevereiro de 2019, que fornecesse informações sobre quem transitou por determinados locais da cidade do Rio de Janeiro/RJ, a partir dos dados de busca e de acesso em seus aplicativos.

O Ministério Público do Rio de Janeiro pretendia obter dados de geolocalização de todos os usuários que encontravam-se nas imediações de onde foi visto o automóvel utilizado pelos atiradores em um intervalo de quinze minutos, bem como os usuários que realizaram buscas no Google procurando por determinados termos específicos ("Marielle Franco", "vereadora Marielle", "agenda Marielle", "agenda vereadora Marielle", "Casa das Pretas", "Rua dos Inválidos 122" e "Rua dos Inválidos") até cinco dias antes do crime.

O Google defende que, no ordenamento jurídico brasileiro, não se admitem quebras de sigilo e interceptações genéricas, sem a individualização das pessoas afetadas. A provedora alegou ainda que a medida, determinada de forma genérica, é desproporcional. A empresa defende que a questão em jogo é que fornecer esses dados à investigação viola a privacidade de milhões de usuários que nada tinham a ver com o crime para poder chegar aos culpados[30].

---

[29] "Para Beccaria, a utilidade é algo material e concreto, pleno de conteúdo axiológico. Nesta acepção, útil é unicamente aquilo que está a serviço dos direitos da maioria e visa garantir a máxima felicidade ao maior número, o que confere ao conceito uma dimensão adequada às perspectivas jurídicas liberais-burguesas da época" (FREITAS, Ricardo de Brito A. P. Razão e sensibilidade: fundamentos do direito penal moderno. São Paulo: Juarez de Oliveira, 2001, p. 76).

[30] STJ manda Google ceder dados de usuários para investigar morte de Marielle. 26/08/2020. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/08/26/google-x-mp-stj.htm?cmpid=copiaecola> Acesso em: 16 mar. 2021

Por maioria, o STJ negou provimento ao recurso[3132] e manteve a decisão que determinou à empresa o fornecimento de informações de usuários de seus serviços no âmbito das investigações. Segundo o ministro Rogerio Schietti Cruz, relator,

> "para a quebra do sigilo de dados armazenados, de forma autônoma ou associada a outras informações pessoais, a autoridade judiciária não é obrigada a indicar previamente as pessoas que estão sendo investigadas, mesmo porque o objetivo da medida é justamente proporcionar a identificação de usuários do serviço ou de terminais utilizados"[33]

Em razão da amplitude da ordem mencionada no caso Marielle Franco, junto com os dados pessoais, inclusive dados de comunicações, dos possíveis suspeitos, o Ministério Público disporá dos dados de qualquer indivíduo que esteve próximo à cena do crime e de qualquer indivíduo que tenha feito pesquisas sobre quaisquer das referidas palavras-chave, mesmo que não tenha relação alguma com o crime em questão – indivíduos que possivelmente buscaram o nome da vereadora por serem partidários de suas ideias, por exemplo, ou mesmo pessoas que estivessem nas imediações do centro do Rio de Janeiro naquela noite.

Nesse amplo cenário de investigações, na diligência de encontrar algum suspeito, viola-se a privacidade de centenas ou até milhares de usuários, além do sério risco de serem injustamente levados à investigação criminal em razão da geolocalização ou de buscas online registradas por seus dispositivos[34]. O grande desafio em torno da matéria é conciliar, de um lado, a necessária segurança jurídica para as autoridades se utilizarem de dados pessoais no âmbito de suas atividades, e, de outro lado, garantir aos cidadãos que seus dados pessoais não sejam usados de modo abusivo, equivocado ou discriminatório pelo estado.

Para elucidar o tema, é válido observar a experiência internacional. Nos Estados Unidos, até o ano de 2015, havia posicionamento jurisprudencial no sentido de que o usuário não tem uma razoável expectativa de privacidade sobre seus dados de geolocalização, já que os utiliza em seus dispositivos a todo momento e concordou com suas políticas de privacidade.

Esse cenário foi alterado quando da adoção da prática de *geofencing* - ou busca reversa - por agentes federais americanos, em 2016, na Carolina do Norte e que se espalhou

---

[31] O número deste processo não é divulgado em razão de segredo judicial.
[32] Terceira Seção rejeita recurso da Google contra fornecimento de dados no caso Marielle Franco. Site oficial do Superior Tribunal de Justiça. <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/26082020-Terceira-Secao-rejeita-recurso-da-Google-contra-fornecimento-de-dados-no-caso-Marielle-Franco.aspx>
[33] Ibidem
[34] ABRUSIO et al., 2020, p. 2.

para estados como California, Flórida, Minnesota e Washington[35]. Um caso específico chamou a atenção da imprensa americana quando cobriu, em dois mandados, uma área equivalente a 3 hectares em um período de 9 horas, obrigando o Google a entregar à polícia federal americana dados de cerca de 1.500 dispositivos armazenados em um banco de dados chamado Sensor Vault[36]. O tema voltou aos holofotes em casos relevantes como o Cambridge Analytica[37] e em normativos recentes, como o California Consumer Privacy Act[38].

Frente ao espanto que os números de *geofencing* tem causado, inclusive em membros do Congresso Americano[39], é inevitável que surjam demandas judiciais específicas revisitando o tema da expectativa de privacidade dos usuários diante da nova cultura de tratamento de dados que se desenvolve no país. Nesse sentido, a Suprema Corte Americana, em 2018, proferiu decisão no sentido de que é necessário mandado específico para obtenção de dados de conexão de dispositivos próximos a cenas de crime por companhias de telecomunicações em Carpenter v. Estados Unidos[40].

No contexto de combate ao terrorismo na Europa, que se intensificou após os atentados de Londres em 2005, foi editada a Diretiva 2006/24 (Diretiva de Retenção de Dados), que passou a exigir que companhias de telecomunicações devem manter, por pelo menos seis meses, os registros de dados pessoais de seus usuários para sua eventual utilização em investigações criminais. Entretanto, esse impulso foi contido em razão das sérias violações à privacidade que a Diretiva representava aos cidadãos[41].

Em razão disso, a Diretiva de Retenção de Dados foi invalidada em abril de 2014 pelo Tribunal de Justiça da União Europeia, com fundamento na proteção à privacidade, considerando investigações não podem ser indiscriminadas, mesmo quando têm por objetivo combater infrações graves como o terrorismo. Portanto, mesmo a grave ameaça do terrorismo

---

[35] The New York Times. Tracking phones, Google is a dragnet for the police. 13/04/2019. Disponível em https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html

[36] Forbes. Google hands Feds 1,500 phone locations in unprecedented 'geofence' search. 11/12/2019. Disponível em https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leads-to-arsonist-smartphones-in-unprecedented-geofence-search/#6e915d4127dc

[37] Facebook sued by Australian information watchdog over Cambridge Analytica-linked data breach. Disponível em https://www.theguardian.com/news/series/cambridge-analytica-files.

[38] Texto na íntegra em: https://oag.ca.gov/privacy/ccpa.

[39] Ver https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Google.2019.4.23.%20Letter%20to%20Google%20re%20Sensorvault.CPC_.pdf

[40] WASSOM, Briam. Augmented reality law, privacy, and ethics: law, society and emerging AR technologies. Waltham: Elsevier, 2015, p.67.

[41] A exemplo, https://www.zeit.de/datenschutz/malte-spitz-data-retention

é insuficiente para justificar uma atuação de vigilância generalizada sobre os usuários de telecomunicações (*dragnet surveillance*).

A harmonia entre o uso de dados de geolocalização em investigações criminais e a observância do direito à privacidade dos usuários – que, em regra, não terão relação com a atividade criminosa- deve necessariamente passar pelo estabelecimento de critérios de proporcionalidade que impeçam a vigilância em massa[42], restringindo a análise aos dados pessoais dos investigados.

Nada obstante, deve-se garantir a qualidade dos dados, para evitar que a investigação criminal conduza a conclusões equivocadas, a exemplo do recente episódio, na Dinamarca, em que 32 presos foram libertados em razão de falhas em indícios de geolocalização de telefones celulares. Em tal caso, a própria polícia detectou falhas de em processos de conversão de dados que tornavam os registros de ligações e de geolocalizações incompletos, além de sistemas que detectavam dispositivos conectados ao mesmo tempo a diversas estações de rádio-base" a quilômetros de distância umas das outras[43].

Cumpre, ainda, destacar a distinção feita pela justiça alemã entre interceptação de telecomunicação e infiltração online. Essa distinção decorre especialmente de um julgado do Tribunal Constitucional Alemão de 2008 que versava sobre infiltrações online (Online-Durchsuchung)[44] e da consequente alteração do código de processo penal alemão (Strafprozessordnung – StPO) em seu § 100b[45], em 2017. Assim como em 1983, no famoso julgado do censo, no qual o Tribunal constitucional alemão criou o direito fundamental à autodeterminação informativa, no julgado de 2008 sobre investigações online, o tribunal criou outro direito fundamental nomeado como "Direito fundamental da garantia da confidencialidade e integridade dos sistemas de tecnologia da informação".

---

[42] DUARTE, Fábio; FIRMINO, Rodrigo. Espaço, visibilidade e tecnologias: (Re)caracterizando a experiência urbana IN Vigilância e Visibillidade: espaço, tecnologia e identificação. São Paulo: Ciber Cultura, 2010.
[43] The Guardian. Denmark frees 32 inmates over flawed geolocation revelations. 12/09/2019. Disponível em https://www.theguardian.com/world/2019/sep/12/denmark-frees-32-inmates-over-flawed-geolocation-revelations
[44] BVerfGE 120, 274 – 350. A proteção reconhecida pela Corte Constitucional alemã em 2008 incide em casos que compreendem sistemas informacionais que contenham dados pessoais de determinado indivíduo, de modo a criar um perfil em violação à sua pessoa. Por essa decisão são reconhecidos novos riscos à personalidade do indivíduo, extinguindo a linha divisória que separava o corpo físico do 'corpo eletrônico'. Não há mais objetos distintos de proteção, mas um único: a pessoa em suas várias configurações, gradualmente determinada por sua relação com as tecnologias.
[45] Redação completa do dispositivo, em alemão: https://www.gesetze-im-internet.de/stpo/__100b.html

O primeiro julgado diz respeito ao acúmulo de dados pela administração estatal, já o segundo versa sobre o acúmulo de dados pelo estado para investigação penal. Em virtude da potencialidade lesiva maior de investigações baseadas em dados pessoais, há, no contexto alemão, uma necessidade maior de justificação de medidas (e reserva legal qualificada) em detrimento do processo dentro do regime jurídico das telecomunicações (por exemplo, interceptação telefônica), pois a primeira abre um leque maior de possibilidade ao se criar perfis completos de indivíduos[46].

Voltando ao caso Marielle Franco, o procurador do MP-RJ Orlando Belém discordou do Google e destacou que as autoridades não veem prejuízo à privacidade na requisição de dados. "Há uma proporcionalidade, já que não conseguimos ter elementos indicativos para encontrar a autoria intelectual do crime. Há uma necessidade efetiva e um interesse público para o reconhecimento e a concessão da ordem".

Em seu voto[47], o relator do caso no tribunal, ministro Rogério Schietti Cruz disse que o pedido de dados é diferente de uma interceptação telefônica, servirá para apurar "gravíssimos crimes", e que os dados de pessoas que forem cedidos pelo Google não serão tornados públicos.

O relator, ministro Rogério Schietti Cruz, disse em junho que o assunto vai muito além da investigação a respeito de Marielle Franco, pois há um "aparente confronto entre o direito à privacidade dos indivíduos e o interesse público na atividade de persecução penal e de segurança pública"[48][49], e completa:

> "[A definição de parâmetros sobre esse tema] ganha especial importância diante do desenvolvimento atual das tecnologias e do aumento de práticas delituosas que dependem, cada vez mais, das informações coletadas pelos diversos tipos de aplicativos ou de redes sociais, as quais têm sido cada vez mais exploradas pelos

[46] Não fosse esse alargamento, seria possível que uma autoridade que tivesse acesso a determinado sistema pudesse ter conhecimento de um extenso conjunto de dados, sem estar submetido a limites acerca do seu tratamento. Sobre o assunto veja Gabriele Britz, Freie Entfaltung durch Selbstdarstellung. Mohr Siebeck, Tübingen 2007, p. 51 ss. E ainda, veja Fabiano Menke, A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) Gilmar Ferreira Mendes; Ingo Wolfgang Sarlet; Alexandre Zavaglia P. Coelho. Direito, inovação e tecnologia. v.1. São Paulo: Saraiva, 2015, p.205.

[47] Terceira Seção rejeita recurso da Google contra fornecimento de dados no caso Marielle Franco. Site oficial do Superior Tribunal de Justiça. <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/26082020-Terceira-Secao-rejeita-recurso-da-Google-contra-fornecimento-de-dados-no-caso-Marielle-Franco.aspx>

[48] Terceira Seção vai decidir sobre fornecimento de dados pelo Google na investigação do caso Marielle. Site oficial do Superior Tribunal de Justiça. 10/06/2020. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Terceira-Secao-vai-decidir-sobre-fornecimento-de-dados-pelo-Google-na-investigacao-do-caso-Marielle.aspx>

[49] O número deste processo não é divulgado em razão de segredo judicial.

> meios investigativos no âmbito do processo penal.” (Rogerio Schietti Cruz, ministro do STJ)[50]

Danilo Doneda[51] acredita que essa abordagem de investigação colocaria pessoas inocentes em uma situação mais frágil perante a justiça. Nas palavras do jurista, "Ficam sujeitas a engano, azar, para serem investigadas. Isso potencialmente pode até diminuir a qualidade da investigação".

Na mesma linha, esclarece Francisco Brito Cruz[52], diretor do centro de direito digital Internetlab: "Não é só porque ferramentas tecnológicas existem que elas têm que servir para o propósito de investigação.” Segundo Cruz, se o STJ adotasse a tese do MP-RJ, ele estaria estendendo bastante a interpretação de quais registros podem ser requeridos em detrimento de direitos fundamentais.

[50] Ibidem
[51] Nota para UOL, Coluna Tilt, de Rodrigo Trindade [Internet]. São Paulo, 26/08/2020. Disponível em: < https://www.uol.com.br/tilt/noticias/redacao/2020/08/26/google-x-mp-stj.htm#:~:text=Em%20seu%20voto%2C%20o%20relator,Google%20n%C3%A3o%20ser%C3%A3o%20tornados%20p%C3%BAblicos.>
[52] Ibidem

4 RUMO A UMA LEI DE PROTEÇÃO DE DADOS NA SEGURANÇA PÚBLICA NO BRASIL

A legislação para a proteção a dados pessoais na sociedade informatizada é uma preocupação que remonta, pelo menos, a 1981, quando foi concluída a Convenção do Conselho da Europa para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal (ETS 108[53]). Em 1995, a União Europeia aprovou sua principal Diretiva sobre Proteção de Dados (95/46/CE[54]).

Diante da nova dinâmica digital criada pela internet, em 2016, o Parlamento e o Conselho Europeu adotaram o Regulamento (UE) nº 2016/679, conhecido internacionalmente por GDPR (sigla de General Data Protection Regulation, ou Regulamento Geral sobre Proteção de Dados), que veio para aperfeiçoar a proteção de dados pessoais na União Europeia, garantir sua livre circulação entre os Estados-membros do bloco e regular sua transferência a Estados terceiros (non-EU) e a organizações internacionais.

Aprovada simultaneamente, a Diretiva nº 2016/680[55], conhecida como Diretiva Policial, regula a proteção de dados em relação ao tratamento de dados pessoais pelas autoridades policiais para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e a livre circulação desses dados.

Ao mesmo tempo, e tomando como base a atuação europeia, outros países seguiram o mesmo caminho. À vista das intensas relações econômicas, culturais e jurídicas mantidas com o continente europeu, o Brasil não poderia se eximir de regular no ordenamento pátrio esse conjunto de direitos e obrigações. Em 2018, o Congresso Nacional aprovou a Lei Geral de Proteção de Dados (Lei n. 13.709/2018), fortemente inspirada no GDPR. Contudo, o legislador brasileiro resolveu postergar a regulamentação da proteção de dados pessoais no âmbito da segurança pública e da persecução penal.

---

[53] Em inglês, a European Treaty Series nº 108. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37>

[54] Texto da Diretiva em inglês. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14012>

[55] Redação na íntegra, em português lusitano. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=PT>

4.1. O anteprojeto da LGPD Penal

A despeito de a LGPD ter excluído de seu próprio escopo as operações de tratamento de dados pessoais voltadas a fins de segurança pública e investigação e repressão de infrações penais, não se pode dizer que estas aplicações não possam gerar riscos jurídicos, seja pela potencial violação de disposições da Constituição, seja por conflito com normas legais existentes.

A vista disso, uma comissão de juristas liderada pelo ministro Nefi Cordeiro, do Superior Tribunal de Justiça, foi entregue em novembro de 2020 ao presidente da Câmara, Rodrigo Maia (DEM-RJ), anteprojeto de lei, ficou conhecido como "LGPD Penal", que disciplina a proteção de dados pessoais em investigações criminais e de segurança pública.

O tema já era discutido e exigido pela LGPD e era uma necessidade da jurisprudência, assim como ocorreu em todo o ocidente. Tivemos de discutir, por exemplo, o uso como prova de prints do Whatsapp web[56], propostas discursando sobre vírus instalado pela polícia no celular de suspeitos[57], discussão do acesso a dados de celulares[58], etc.

Vivemos uma concreta necessidade de que Judiciário resolva esses conflitos, do alcance da proteção à privacidade dos cidadãos em procedimentos criminais. Por outro lado, há uma necessidade de que o judiciário tenha um suporte mais estável, mais representativo dos desejos sociais, e daí necessidade da edição dessa lei.

O fato é que o crime se moderniza. As novas tecnologias de informação e interação que influenciam diversas áreas das atividades econômicas, sociais, culturais e políticas acabam por também ensejar o aparecimento de novos crimes. Impressiona a capacidade de adaptação dos agentes criminosos às novas tecnologias, com modificação quase que instantânea, por exemplo, de seus *modus operandi* para fazer frente a novos padrões de segurança de empresas

---

[56] Print de conversa pelo WhatsApp Web não é prova válida, reafirma STJ. Revista Consultor Jurídico. 9 de março de 2021 https://www.conjur.com.br/2021-mar-09/print-conversa-whatsapp-web-nao-prova-valida-reafirma-stj

[57] PF quer instalar vírus em telefone grampeado para copiar informações. Jornal Folha de São Paulo. 27/04/2015. https://m.folha.uol.com.br/poder/2015/04/1621459-pf-quer-instalar-virus-em-telefone-grampeado-para-copiar-informacoes.shtml

[58] AGRAVO REGIMENTAL NO HABEAS CORPUS. TRÁFICO DE DROGAS. NULIDADE. ACESSO AOS DADOS DO APARELHO CELULAR DO RÉU. PRÉVIA ORDEM JUDICIAL. CONSTRANGIMENTO ILEGAL NÃO VERIFICADO. AGRAVO REGIMENTAL IMPROVIDO. 1. Esta Corte Superior de Justiça considera ilícito o acesso a dados do celular apreendido em flagrante, quando ausente ordem judicial para tanto, pela violação dos direitos de privacidade. 2. Caso em que o acesso a mensagens e dados extraídos do celular do agravante ocorreu com prévia autorização judicial, inexistindo ilegalidade a ser reconhecida. 3. Agravo regimental improvido. (AgRg no HC 598.960/SC, Rel. Ministro NEFI CORDEIRO, SEXTA TURMA, julgado em 20/10/2020, DJe 26/10/2020)

ou instituições, bem como a dinâmica plasticidade de suas empresas de fachada, com alteração de local e área de atuação, troca de colaboradores, remoção de pessoal para agirem em locais ainda não atingidos, utilização de novas contas bancárias com nomes falsos e a infindável troca de telefones de contato.

Nessa perseguição à "modernização dos riscos", temos precisado enfrentar situações sem suporte legal com a criação de limites estabelecidos pelo Judiciário e até pelo próprio Superior Tribunal de Justiça, que precisam ser bastante sopesados porque refletem uma concepção dos juízes para os casos concretos e que podem eventualmente não ser o melhor caminho para a sociedade.

Conforme Lodder (2020, p. 132) se o bom resultado das investigações – em especial os delitos financeiros e os praticados por organizações criminosas – depende do uso e tratamento de dados pessoais[59], seria contraproducente e prejudicial à própria sociedade que aos órgãos investigadores fosse vedada a legitimidade para fazê-lo.

O anteprojeto de lei, que é chamado de "LGPD Penal", tem o seu motivo, pois, analisando o art. 4º da LGPD, onde constam as situações onde a lei não se aplica:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
>
> [...]III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais;

O §1º do artigo em comento indica que essa temática deverá ser objeto de legislação específica. Dentre as quatro situações descritas no art. 4º, a medida se aplica ao tratamento de dados por autoridades competentes em atividades de segurança pública e persecução penal enquanto veda, no entanto, sua própria utilização para fins exclusivos de defesa nacional e segurança do Estado.

Dentro dessa perspectiva, segundo a própria exposição de motivos[60], elaborar esta lei adveio diante de uma necessidade prática da modernização das tecnologias na persecução penal ao redor do mundo, compatibilizando o uso das tecnologias pelos órgãos do estado no

---

[59] A propósito, o considerando 27 da Diretiva (UE) n. 2016/680 define: "Para efeitos de prevenção, investigação ou repressão de infrações penais, é necessário que as autoridades competentes tratem os dados pessoais, recolhidos no contexto da prevenção, investigação, deteção ou repressão de infrações penais específicas para além desse contexto, a fim de obter uma melhor compreensão das atividades criminais e de estabelecer ligações entre as diferentes infrações penais detetadas."

[60] Disponível em: <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf>

exercício de suas funções de modo eficiente, mas sem perder de vista a observância de garantias processuais e de direitos fundamentais dos titulares dos dados envolvidos.

Ademais, a exposição de motivos do anteprojeto aponta como fatores ensejadores deste debate (i) a falta de adequação aos padrões internacionais de segurança e (ii) a ausência de legislação sobre a licitude, transparência ou segurança do tratamento de dados no âmbito penal. Buscando essa harmonia, de um lado os deveres do estado na prevenção e repressão dos ilícitos, protegendo a ordem pública, e de outro, assegurando a observância das garantias.

Visa, ainda, trazer uma complementação à legislação pátria, a exemplo das leis 12.850/2013 (Lei de Organizações Criminosas), 9.296/1996 (Lei de Interceptações Telefônicas), 12.965/2014 (Marco Civil da Internet), bem como o próprio Código de Processo Civil e outras leis, trazendo um microssistema voltado à proteção de dados na esfera penal e processual penal. Com 12 capítulos e 68 artigos, tem inspiração na Diretiva Europeia 680/16 e também na legislação americana no que tange às tecnologias de alto risco, como as câmeras com reconhecimento facial espalhadas pelas cidades.

O anteprojeto tem base principiológica semelhante à LGPD, mas tem especificidades próprias para esse recorte.

Sobre a proposta apresentada, entende-se que ela se dedica a realizar um debate importante entre atividades de tratamento de dados pessoais e atividades de segurança pública e persecução penal, de modo a harmonizar princípios basilares da proteção de dados pessoais, como a proporcionalidade e a necessidade, às atividades já empregadas pelo Estado[61].

O anteprojeto determina sigilo aos "elementos identificadores" dos dados pessoais de investigados, suspeitos, acusados e condenados sem trânsito em julgado. Como exemplo, será vedado o acesso automatizado e massificado a documentos, tais como provas colhidas, peças processuais, laudos periciais e documentos análogos, com exceção dos atos decisórios.

O texto estabelece que o Poder Judiciário, o Ministério Público e as polícias devem dispor de medidas de segurança aptas a proteger os dados de envolvidos em processos

[61] Coalizão Direitos na Rede. Coalizão Direitos na Rede envia carta aos presidentes do Senado, Davi Alcolumbre, e da Câmara dos Deputados , Rodrigo Maia, em apoio ao anteprojeto de lei sobre proteção de dados em investigações criminais e na área de segurança pública. Brasília, 2020. Disponível em: <https://direitosnarede.org.br/2020/11/09/protecao-de-dados-pessoais-na-seguranca-publica-e-em-investigacoes-criminais/> Acesso em: 18 mar. 2021

criminais. As medidas técnicas e administrativas de segurança deverão ser elaboradas pelo Conselho Nacional de Justiça.

Deverão, ainda, ser criados procedimentos para evitar a utilização, pelas autoridades, de informações pessoais consideradas irrelevantes para o andamento das investigações. Caso esses tipos de dados surjam no decorrer dos processos, eles deverão ser imediatamente descartados.

O anteprojeto determina, ainda, que o uso compartilhado de dados pessoais sigilosos entre autoridades competentes só aconteça com autorização judicial. A disposição é válida, inclusive, para o compartilhamento no âmbito de uma mesma autoridade.

No caso, um dos mecanismos limitadores do poder de polícia do Estado está presente no Capítulo VI do Anteprojeto que determina a obrigação das autoridades competentes de fornecer informações claras e atualizadas sobre a base legal, a finalidade, os objetivos específicos, os procedimentos e as práticas utilizadas para a execução de suas atividades (art. 40).

Além disso, em consonância com a principiologia da LGPD, o anteprojeto salienta a importância dos princípios da responsabilização e prestação de contas, destacando como obrigação dos agentes de tratamento a elaboração de relatórios de impacto à proteção de dados pessoais em caso de tratamento de dados sensíveis, sigilosos ou operações de elevado risco para os direitos, liberdade e garantias dos titulares (art. 42, Capítulo VIII).

Aprovada, a LGPD Penal ainda poderá trazer parâmetros para o uso adequado e legítimo da tecnologia na atividade policial, visto que definirá como tais mecanismos poderão auxiliar autoridades a alcançarem a finalidade de segurança pública observando direitos fundamentais. Nessa medida, destaca-se positivamente a congruência terminológica e conceitual do anteprojeto com a LGPD, imprescindível para garantir segurança jurídica no novo quadro regulatório da proteção de dados no país.

Ainda, estabelece remédios, como o tipo penal da “Transmissão ilegal de dados” (Art. 66), que pode contribuir para coibir potenciais abusos de poder por parte daqueles que tratam dados pessoais.

Houve grande discussão - que, pela relevância do tema, ainda não pacífica - sobre quem seria a autoridade nacional para o controle do tratamento de dados na segurança pública, inclusive para termos acesso a informações e providências policiais e persecutórias

internacionais, já que a autoridade nacional brasileira atualmente, nos limites da LGPD, teria sérias discussões quanto a sua independência e autonomia. Por essa razão, surge a ideia do Conselho Nacional de Justiça como grande controlador dos dados penais, o que não parece ser o modelo ideal, mas foi o que se encontrou como mais viável para a realidade brasileira para que se tenha uma autoridade com autonomia e especialização para tal controle.

A Coalizão Direitos na Rede, coletivo que reúne mais de 40 entidades da sociedade civil e organizações acadêmicas que trabalham em defesa dos direitos digitais, enviou, em novembro de 2020, carta[62] aos presidentes do Senado, Davi Alcolumbre, e da Câmara dos Deputados , Rodrigo Maia, em apoio ao anteprojeto:

> "Adicionalmente, é importante mencionar que o anteprojeto de lei está alinhado com iniciativas e discussões internacionais relacionadas ao tratamento de dados pessoais para fins de atividades de segurança pública, como a Diretiva n. 2016/680 do Parlamento Europeu. Nesse sentido, a aprovação de um projeto de lei sobre o tema em questão, além de mais um passo importante para o Brasil no campo de proteção de dados pessoais, facilitaria atividades de cooperação jurídica internacional, sobretudo em matéria penal.
>
> Assim, as entidades que integram a Coalizão Direitos na Rede esperam contar com o apoio do Congresso Nacional para a promoção de uma discussão participativa sobre o anteprojeto com todos os setores interessados e sua posterior aprovação. Longe de inviabilizar investigações e eventuais responsabilizações de agentes que violem as leis em vigor no país, o Parlamento brasileiro confirmaria assim seu compromisso com a defesa e garantia dos direitos fundamentais de todos os cidadãos e cidadãs."

4.2. Questões sensíveis na proteção de dados em investigações criminais

Em que pese as entidades da sociedade civil organizada se manifestarem publicamente em apoio à proposta de criação de uma LGPD Penal, por outro lado, o texto foi recebido criticamente por representantes de entidades de classe associadas ao sistema de justiça criminal, como delegados da polícia federal e promotores.

Conforme apontado alhures, a Comissão de Juristas responsáveis pelo anteprojeto foi fortemente influenciada pela Diretiva 680/2016, do Parlamento Europeu e do Conselho Europeu, de abril de 2016.

Ocorre que uma simples leitura comparativa entre o texto apresentado pela Comissão de Juristas e a normativa europeia evidencia inegável descompasso, notadamente em relação aos objetivos normativos e às dimensões do tratamento dos dados pessoais[63].

---

[62] Ibidem

[63] MARQUES et al. O anteprojeto da 'LGPD penal' e a (in) segurança pública e (não) persecução penal. Site Jota. 09/12/2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-anteprojeto-da-lgpd-penal-e-a-in-seguranca-publica-e-nao-persecucao-penal-09122020>

A Diretiva (EU) 2016/680 enuncia expressamente seus objetivos, quais sejam os de (i) proteger os direitos e liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção de dados pessoais, e (ii) assegurar o livre intercâmbio desses dados pelas autoridades competentes na União Europeia (Considerando 93).

Para a concretização desta dupla finalidade, o sistema estruturado pela Diretiva Europeia alcança o tratamento de dados pessoais realizado pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública (artigo 1º, 1).

O texto do anteprojeto, por seu turno, embora influenciado pela Diretiva (EU) 680/2016, apenas importou as lógicas da investigação e repressão de infrações penais, mas omitiu-se quanto a importantíssimos pilares da prevenção e da detecção de condutas delitivas, que demandam a utilização de dados em massa, em ambientes restritos e controlados.

E mais. Ao invés de estabelecer balizas para o intercâmbio de dados entre as autoridades competentes, o anteprojeto estabelece restrições consideradas desproporcionais e distantes da realidade, como as previstas nos artigos 14, § 2º[64], 43[65] e 45[66], "sem oferecer, em contrapartida, uma melhoria palpável dos direitos das pessoas em causa" (MARQUES et al., 2020).

Destaca-se a excessiva amplitude do conceito de dado pessoal, entendido como qualquer "informação relacionada a pessoa natural identificada ou identificável" (art. 5º, inciso I), disponibilizada em "suporte eletrônico ou físico" (art. 5º, V). Nesse contexto, não causa estranheza que o anteprojeto tenha incorrido em confusão conceitual que pretende atribuir natureza probatória a todo "dado pessoal", ignorando que em boa parte dos casos o manejo de

---

[64] Art. 14. O tratamento de dados pessoais sigilosos somente poderá ser realizado se estiver previsto em lei e para atividades de persecução penal.
§2º. O acesso a dados pessoais sigilosos controlados por pessoas jurídicas de direito privado será específico a pessoas investigadas e dependerá de ordem judicial prévia baseada em indícios de envolvimento dos titulares de dados afetados em infração penal e na demonstração de necessidade dos dados à investigação, na forma da lei.
[65] Art. 43. O uso compartilhado de dados pessoais entre uma autoridade competente e outro órgão ou entidade do Poder Público não competente para os fins desta Lei dependerá de autorização legal específica, sendo vedadas hipóteses em que o tratamento posterior seja incompatível com a finalidade original da coleta, em termos de expectativas legítimas de titulares de dados ou de objetivos de políticas públicas que ensejaram a coleta original.
[66] Art. 45. É vedado a pessoas jurídicas de direito privado praticar modalidades de uso compartilhado de dados com autoridades competentes, exceto nas hipóteses específicas previstas em lei ou mediante cooperação voluntária, desde que observadas as demais disposições dos Capítulos I e II desta Lei e da Lei nº 13.709/18.

dados, sobretudo nos campos da prevenção e da detecção de infrações penais, serve ao propósito de orientar a atuação dos órgãos de persecução e auxiliar na prospecção de trilhas investigativas.

Assim, ao pretender regular todos os aspectos referentes ao tratamento de dados pessoais, físicos ou eletrônicos, na persecução penal e na segurança pública, o anteprojeto impacta diretamente temas regulados por outros diplomas, como o da prova penal e das técnicas especiais de investigação, causando embaraços ao processo penal[67].

Em "alerta geral à nação", as entidades apontam que o texto do anteprojeto está repleto de vícios de inconstitucionalidade, e outras normas que inviabilizam os trabalhos na área[68].

De acordo com o documento, uma das normas mais graves propostas pelo anteprojeto é a transformação do Conselho Nacional de Justiça – CNJ em órgão de controle externo de acesso aos dados pelos profissionais de segurança pública. Dentre as atribuições do CNJ, conforme definido pela Constituição Federal, não se encontra a atividade de controle externo das polícias e das forças de segurança pública. O controle externo da Polícia Judiciária é, por lei, função do Ministério Público.

O anteprojeto pretende, ainda, criar um "intermediário administrativo controlador"[69], que atuará entre a autoridade que elabora as investigações e a empresa privada que faz o tratamento dos dados de interesse. Com isso, acaba por criar uma nova burocracia que pode dificultar as ações policiais.

Considerando o princípio da reserva de lei e partindo da ideia de que há que se conciliar interesses persecutórios com interesses individuais e que aqueles só são legítimos se estiverem previstos em lei, a "medida do possível" é a medida da lei. Inadequada, portanto, nos arts. 7º e 8º, a previsão da expressão "na medida do possível", já que pode sugerir que há uma margem de discricionariedade na atuação e na intervenção na proteção de dados. Sem prejuízo do que está disposto no anteprojeto, a expressão poderia simplesmente ser suprimida[70].

---

[67] Nota técnica elaborada pela Secretaria de Perícia, Pesquisa e Análise (SPPEA) da Procuradoria-Geral da República (PGR). Disponível em: <https://criminal.mppr.mp.br/arquivos/File/ENCCLA_-_PGR-00456556-2020_NT.pdf>

[68] Entidades publicam alerta contra anteprojeto da LGPD Penal em estudo na Câmara. Site Jota. 15/12/2020. Disponível em: <https://www.jota.info/jotinhas/lgpd-penal-seguranca-publica-anteprojeto-15122020>

[69] Art. 5º Para os fins desta Lei, considera-se:I X - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e o Conselho Nacional de Justiça (CNJ);

[70] LEITE, Alaor. Webinário Proteção de Dados, segurança pública e persecução penal. [jan. 2021]. Instituto LGPD – Legal Grounds for Privacy Design. Brasil, 2021. Youtube (141 min.)

Vê-se com preocupação o art. 9º, pelo desatendimento ao princípio básico da reserva legal. As exigências de uma reserva de lei que, no Brasil, já advém do art. 5º, II da CF, e no próprio anteprojeto, do art. 2º, VII[71], não são em nada atendidas pelo art 9º, já que permite uma regulamentação da proteção de dados por via regulamentar, e não por lei em sentido formal. Uma lei de proteção de dados que prevê este art. 9º falha num aspecto central e abandona em boa parte qualquer ideia de proteção de dados mais ambiciosa.

A lei não deixa claro como se dá a obtenção dos dados, ou seja, como esses dados chegam ao conhecimento do estado. O normativo parece pressupor que os dados já chegaram ao conhecimento do Estado. É certo que chegam até o estado de diversas formas, mas o que se discute é como se dá a transferência deles para a persecução penal e como a própria persecução penal vai chegar ao conhecimento de novos dados, já que a questão da proteção dos dados se inicia com a sua obtenção. Como exemplo, continuam existindo no direito brasileiro, na Lei 12.850/2013, os arts. 16, 17 e 18, que exigem que as companhias telefônicas devem manter dados de telecomunicação por 5 anos.

O anteprojeto da LGPD Penal, em seu artigo 15, inciso 1º, diz que "é vedado o acesso automatizado e massificado a quaisquer documentos". Em tese, isso acabaria com a consulta eletrônica de processos, popularizada pela 13ª Vara Federal durante a Lava Jato. Diante disso, as entidades defendem que

> "a atividade de segurança pública depende em seus trabalhos de análises de dados em massa, feitas de maneira impessoal e profissional, de acordo com protocolos doutrinários próprios e que devem convergir com a legalidade e respeito à privacidade, mas que são extremamente eficazes nas chamadas investigações proativas".

No art. 20, III, uma hipótese de recusa do acesso aos dados é quando há interesse de defesa nacional ou segurança do Estado. Note-se que esses interesses não vêm definidos nesta lei, tampouco na legislação esparsa, e a utilização desses motivos pode muito habilmente ser utilizada para violar o direito de acesso aos dados pelos titulares afetados. São interesses etéreos, por vezes muito graves e concretos, mas se assim o é, necessita-se dizer quando esses interesses de defesa e segurança nacional são suficientemente concretos para que suplantem o direito individual que o sujeito tem de acessar o que o Estado sabe sobre ele.

---

[71] Art. 2º A disciplina da proteção de dados pessoais em atividades de segurança pública e de persecução penal tem como fundamentos: [...] VII - garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal.

Aponta-se, também, que o anteprojeto fere a Lei 12.850/2013, em seu artigo 15, e a Lei de Lavagem de Dinheiro, nº 9.613/98, em seu artigo 17-B, que estabelecem acesso aos dados pela autoridade policial e o Ministério Público, independente de autorização judicial. O artigo 45 do anteprojeto se debruça sobre uso compartilhado de dados pessoais entre autoridades competentes, mas coloca ao lado da autorização legal a hipótese de autorização judicial. Com isso, acaba eternizando uma argumentação ainda muito comum, mas que é circular, de que a autorização judicial sanava o compartilhamento não autorizado em lei de dados entre órgãos estatais.

A autorização judicial deve se basear em um instrumento legislativo, vez que não existe como tal, não podendo sanar violações prévias às regras que devem orientar o compartilhamento de dados. Ora, se é o princípio da reserva legal que orienta este projeto, ele não pode conceder hipóteses de uma autorização judicial sem que haja correspondente autorização legal. A grande dificuldade é que, como o anteprojeto é um instrumento inaugural, e não existem essas autorizações legais prévias em nosso processo penal, ele está inserido num dilema a ser equilibrado, mas não é possível deixar-se de atentar para este fato.

Da forma em que se encontra, o texto pode ser aplicado para impedir, por exemplo, o compartilhamento direto de dados entre o Coaf e a Receita com o Ministério Público e a Polícia Federal. O que contraria decisão do plenário do Supremo[72] que, no ano passado, derrubou a polêmica liminar de Dias Toffoli, que chegou a suspender por meses o inquérito da rachadinha envolvendo Flávio Bolsonaro e todas as investigações do país baseadas em dados do Coaf. Na ocasião, por 9 votos a 2, o plenário autorizou o compartilhamento desses relatórios.

Aparentemente, a regra é uma vedação ao compartilhamento entre órgãos de segurança pública e órgãos de persecução penal, mas o art. 45, §1º, II cria uma exceção a essa regra, permitindo esse compartilhamento, desde que ele se destine a uma investigação criminal

[72] Ementa Repercussão geral. Tema 990. Constitucional. Processual Penal. Compartilhamento dos Relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil com os órgãos de persecução penal para fins criminais. Desnecessidade de prévia autorização judicial. Constitucionalidade reconhecida. Recurso ao qual se dá provimento para restabelecer a sentença condenatória de 1º grau. Revogada a liminar de suspensão nacional (art. 1.035, § 5º, do CPC). Fixação das seguintes teses: 1. É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil - em que se define o lançamento do tributo - com os órgãos de persecução penal para fins criminais sem prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional; 2. O compartilhamento pela UIF e pela RFB referido no item anterior deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios. (RE 1055941, Relator(a): DIAS TOFFOLI, Tribunal Pleno, julgado em 04/12/2019, PROCESSO ELETRÔNICO DJe-243 DIVULG 05-10-2020 PUBLIC 06-10-2020 REPUBLICAÇÃO: DJe-052 DIVULG 17-03-2021 PUBLIC 18-03-2021)

específica. Ocorre que esse é justamente o único caso em que esse compartilhamento é problemático, ou seja, o que é construído sob a forma de uma vedação é, na verdade, uma autorização de compartilhamento, pois é evidente que polícias e Ministério Público apenas solicitarão esse compartilhamento, com ou sem intermediação judicial, caso já haja linha investigatória contra sujeitos em específico. Nesse sentido, esse pressuposto já atenderia à exceção à vedação. Na ótica deôntica das normas, o que era uma vedação, se torna uma autorização geral.

Diz-se, portanto, que é preciso aprofundar as convicções do próprio anteprojeto no sentido de entender que órgãos de segurança pública tem uma finalidade que não se confunde com a persecução penal e que, portanto, uma criação direta ou indireta de um compartilhamento total de informações não é algo compatível com as ideias reitoras do próprio anteprojeto. Assim, é preciso um cuidado com a redação deste artigo, além do caput, que menciona a autorização judicial.

"O referido anteprojeto está eivado de vícios insanáveis de inconstitucionalidade, ao longo de diversos artigos", defendem a Associação dos Delegados de Polícia do Brasil (ADEPOL), a Associação Nacional dos Delegados de Polícia Federal (ADPF), a Confederação Nacional dos Trabalhadores Policiais Civis (COBRAPOL), a Federação Nacional dos Oficiais Militares Estaduais (FENEME), a Federação Nacional dos Delegados de Polícia Federal (FENADEPOL) e a Federação Nacional dos Delegados de Polícia Civil (FENDEPOL), em documento.

Aduzem as entidades que o texto também cria burocracias avaliadas como desnecessárias, como a elaboração obrigatória de "relatório de impacto à proteção dos dados pessoais", tanto para tratamento de dados pessoais sensíveis, sigilosos ou de operações que apresentem "elevado risco aos direitos, liberdades e garantias dos titulares de dados". Cria, ainda, barreiras que dificultam ou atrasam o compartilhamento de dados entre as polícias, Ministério Público e as empresas privadas detentoras dos dados necessários para a investigação, como informações telefônicas, de cartões de crédito e redes sociais, o que pode acabar por favorecer investigados, que ganharão tempo para eliminar evidências de seus possíveis crimes, e afetando o tempo de resposta da ação policial em casos, por exemplo, em que as vítimas necessitam de resgate[73].

[73] LGPD Penal vai dificultar a investigação policial e favorecer a corrupção e a criminalidade organizada. Estadão, Coluna Fausto Macedo. 17 de dezembro de 2020. Disponível em:

Diante desse embate, e a título de conclusão, faz-se necessário tecer algumas reflexões sobre o tema estudado.

Sem embargo de existirem diferentes pontos de vista sobre a proposta de uma LGPD Penal, e considerando que todos são pertinentes, apesar de conflitantes, incontroverso é que a regulamentação nesse setor é não só urgente, como obrigatória. Não há alternativa à regulação da proteção de dados na persecução penal e segurança pública, e já não o havia antes da Lei 13.709/2018, por imposição constitucional. A alternativa seria o caos[74]. Após a LGPD, há uma recomendação expressa de que se promova uma legislação nesse sentido. De toda maneira, o vácuo nesse setor significa um atraso enorme e um desatendimento a alguns princípios constitucionais que orientam o processo penal brasileiro e que vêm sendo diuturnamente violados.

Ao se colocar uma tarefa desse porte a uma geração, deve-se procurar equilibrar duas situações em uma balança muito sutil: de um lado, os interesses persecutórios legítimos de que fatos puníveis sejam perseguidos e que os culpados sejam condenados criminalmente; de outro, a garantia de que cidadãos inocentes não tenham os seus direitos individuais afetados ilegitimamente.

Essa percepção se torna cada vez mais sensível, e é por isso que a cada medida interventiva no processo penal, a cada nova possibilidade de intervenção na esfera individual, deve ser garantido ao indivíduo afetado um mecanismo compensatório em forma de direito individual. Ordinariamente, as intervenções afetam não apenas aquele que é investigado ou acusado, mas também a terceiro, e essa é talvez a faceta mais dramática da proteção de dados, pois as intervenções em geral, mesmo aquelas feitas por medidas ocultas no processo penal, ocasionalmente atingem terceiros.

O anteprojeto, sabiamente, estipula os direitos de acesso, ao mesmo tempo que, atendendo aos interesses persecutórios, estipula os direitos de recusa ao oferecimento dos dados ao sujeito titular. Essas previsões nos dão uma ideia de que há clareza quanto à posição de titularidade desses dados. Ocorre que, na investigação criminal, não se tem sempre essa clareza.

Não poucas vezes, os órgãos de investigação acabam por retardar a colocação de um sujeito na condição de investigado ou indiciado, justamente para continuar uma linha

<https://politica.estadao.com.br/blogs/fausto-macedo/lgpd-penal-vai-dificultar-a-investigacao-policial-e-favorecer-a-corrupcao-e-a-criminalidade-organizada/>

[74] LEITE, Alaor. Webinário Proteção de Dados, segurança pública e persecução penal. [jan. 2021]. Instituto LGPD – Legal Grounds for Privacy Design. Brasil, 2021. Youtube (141 min.)

investigatória que, naturalmente, acaba por aprofundar a intervenção nos direitos de terceiros, sem que esses terceiros tenham nome no processo. Por isso, diz-se que a investigação criminal se dirige contra determinadas pessoas e acaba afetando outras.

Diante disso, nos parece razoável que a lei também deva dirigir, ressalvadas as medidas que dependem de sigilo, um plexo de direitos a terceiros afetados por essa coleta de dados destinada à persecução penal.

Esse anteprojeto respira uma distinção fundamental que até pouco tempo era desconhecida do processo penal brasileiro, que é a diferença entre persecução penal e segurança pública, conceitos que eram comumente confundidos como se se destinassem à mesma finalidade. Conforme Bioni[75], a ideia de segurança pública está relacionada com o momento pré-crime, ou seja, vinculada à ideia de prevenção, ao passo que a persecução criminal está relacionada à ideia de repressão, na qual já existe um objeto bem definido.

Isso altera visceralmente os pressupostos legais de intervenção. No direito público alemão, solidificou-se a necessidade de se proteger a liberdade dos cidadãos e de limitar a atuação do Estado. A partir da correlação entre poder e saber, é essencial que o acesso às informações (o "saber") seja limitado para que não haja abusos de poder. Na finalidade da segurança pública, o estado deve poder saber mais, mas isso por que ele pode atuar menos concretamente contra um indivíduo em específico. Já no setor da persecução penal, em que o estado está autorizado, inclusive, a medidas cautelares pessoais bastante interventivas, concretas e individualizadas contra uma pessoa em especial, o estado deve poder saber menos, por que ele pode mais. Quem tudo sabe, não deve poder tudo; e quem pode quase tudo, não deve saber de tudo.

Essa divisão fundante do direito alemão é respirada no anteprojeto, contudo, ela não é levada ao seu termo. Há sempre a identificação de que essa proteção de dados deve ser dar tanto no setor da persecução penal, quanto no da segurança pública, porém não há identificação dos pressupostos autorizativos, que são diversos, para uma ou para outra coleta de dados. Nesse sentido, o projeto está animado por essa distinção fundamental, mas está pendente, ainda, de um aprofundamento quanto a essa questão. O anúncio dessa distinção é importante, mas ele ainda não realiza todos os anseios da reserva de lei no processo penal.

Ademais, o tipo penal tipificado no anteprojeto parece ter uma redação defeituosa, pois contém um elemento normativo, que é a transmissão ilegal de dados, o que pressupõe clareza quanto à legalidade dessa transmissão, e essa clareza nao existe. Isso pode conduzir a

[75] BIONI, Bruno. Seminário Internacional da Comissão de Juristas. [jul. 2020]. Câmara dos Deputados (online). 140 min.

dois cenários: ou o tipo penal estará quase sempre realizado, quando houver uma transmissão duvidosa de dados entre órgãos do estado, ou o tipo nunca estará realizado, pois não há uma clareza quanto ao setor primário que o direito penal quer proteger.

Assim, defende-se que a lei necessita das autorizações legislativas no Código de Processo Penal, e sem isso não seria possível pensar numa regulação de dados.

5 CONCLUSÃO

Numa sociedade pautada no mundo virtual, que abrange desde as compras on-line às redes sociais, existe um espaço repleto de informações e dados pessoais que vagam em um universo ilimitado de possibilidades quanto a sua destinação. A partir dessa hiperconectividade, uma vasta quantidade de dados é coletada, processada, compartilhada, tratada e armazenada em bancos de dados utilizados por empresas de tecnologia com as mais diversas finalidades, caracterizando a figura do Big Data[76].

Diante da variedade de informações que chegam em volumes crescentes e com velocidade cada vez maior, o Big Data é uma ferramenta valiosa não só para o mercado tech, mas para o Estado, já que funciona como um navegador entre o emaranhado de dados existentes na rede mundial de computadores. A fim de garantir a transparência e a utilização adequada de dados, principalmente os relacionados à pessoa humana, a LGPD foi criada e entrou em vigor em setembro de 2020.

Centrado no ideal de autodeterminação informativa, isto é, de autonomia e controle do cidadão em relação às informações que o identificam, o novo ambiente regulatório busca harmonizar a proteção dos direitos dos indivíduos e a provisão de segurança jurídica nas relações permeadas pelo tratamento de dados pessoais.

Ainda que a LGPD represente um avanço, há que se considerar a persistência de problemas relativos ao cumprimento desse regramento, bem como o mau uso e a custódia dos dados pessoais. A questão principal abordada neste trabalho de conclusão de curso refere-se ao tratamento dispensado aos dados pessoais quando utilizados pela administração pública tendo em vista a sua utilização na promoção da segurança pública e na persecução penal.

É de se notar que as exigências para a proteção de dados não são fáceis de cumprir. Elas exigem, dentre outras medidas, a elaboração de novas leis e mudanças na própria estrutura organizacional do estado, o que é trabalho para alguns anos. Interessante é que, no setor específico da persecução penal, a decisão do censo alemão ocorreu em 1983 e o legislador precisou de quase 17 anos para proceder a uma regulamentação da proteção de dados dentro de código de processo penal alemão, já que adveio somente em 1999. Uma última reforma veio

[76] Segundo Santos (2019), "o Big Data é mais que um emaranhado de dados, pois é essencialmente relacional. Isso não é novo – para a tristeza daqueles que acreditam que a internet mudou todas as coisas. O que a internet fez foi dar uma nova dimensão a esse fenômeno, transformando-o. Para bem entender essas transformações, precisamos compreender que o Big Data somos nós".

em 2020, para adequar certos aspectos da legislação processual alemã às novas exigências europeias e para adaptar a legislação daquele país para a existência de um processo com autos eletrônicos.

Se, por um lado, o uso de novas tecnologias dentro do processo penal e da investigação criminal garante, certamente, uma maior eficiência e eficácia em manter padrões elevados de segurança pública, por outro, sem um regime adequado de salvaguarda e de garantias individuais adequadas dentro desse processo, pode-se terminar por construir um Estado que exerce constante vigilância, violando direitos e garantias dos cidadãos.

O art. 4º da LGPD excluiu do escopo de aplicação da lei o tratamento realizado para fins exclusivos de segurança pública, defesa nacional, segurança de Estado e investigação e repressão de infrações penais, o que implica na persistência do "direito das quebras de sigilo"[77] enquanto principal referência para a normatização dessas operações de tratamento. Isso pois, embora a lei brasileira tenha forte inspiração no Regulamento Geral de Proteção de Dados da União Europeia, que carrega exceções similares, o Brasil não promulgou uma norma referente ao tema conjuntamente com a LGPD, como ocorreu na Europa. Como resultado, ficou pendente o desenvolvimento de uma norma voltada à segurança pública e persecução penal que se fundamente nos princípios e conceitos contemporâneos do campo da proteção de dados, como o de autodeterminação informativa.

À vista disso, no contexto da demanda pelo desenvolvimento dessa norma, o presidente da Câmara dos Deputados, Rodrigo Maia, determinou em 2019 a criação de uma comissão de juristas voltada a desenvolver um anteprojeto de lei nesse sentido, rapidamente batizado pela mídia de "LGPD penal".

Numa abordagem mais inicial e mais ampla, parece-se que essa proposta de lei realmente precisa de discussão, mas seu anteprojeto, embora provisório e passível de mudanças, representa um marco regulatório na proteção de dados na seara penal, sobretudo pelo grande risco de variadas decisões judiciais em sentidos contraditórios. O que se denota é que é

[77] A despeito da adoção progressiva de tecnologias e procedimentos baseados no tratamento de dados pessoais, o setor de segurança ainda não conta com uma norma que regule extensamente esse tema específico. A pesquisadora Jacqueline Abreu ensina que o que o Brasil possui é uma espécie de "direito das quebras de sigilo", isto é, um conjunto de regras que determina as condições em que dados considerados sigilosos podem ser acessados por autoridades. Composto por normas como a Lei das Interceptações Telefônicas, a Lei Complementar n. 105, o Marco Civil da Internet e o próprio Código de Processo Penal, esse quadro regulatório se fundamenta na tradicional ideia de privacidade como sinônimo de reclusão, um tipo de zona protegida do olhar público. (LGPD penal: um remédio contra o solucionismo tecnológico na segurança pública? - Instituto de Referência em Internet e Sociedade. Nov. 2020. Disponível em: https://irisbh.com.br/lgpd-penal-um-remedio-contra-o-solucionismo-tecnologico-na-seguranca-publica/)

necessário e urgente que se produza um instrumento que compatibilize a defesa dos direitos individuais dos cidadãos brasileiros com a realização do interesse público em matéria de segurança.

Deve-se assegurar que, para cada medida processual penal que interfira na esfera individual, seja garantido ao indivíduo afetado um mecanismo compensatório em forma de direito individual, sobretudo por que, de forma geral, as intervenções afetam não apenas os investigados ou acusados, mas também a terceiros.

Temos, portanto, a grande chance de discutir mais concretamente o alcance desse acesso estatal aos dados dos cidadãos, se vamos ter mais claramente admitida pela jurisprudência a fixação de limites legais com relação ao compartilhamento desses dados e, por conseguinte, um controle dos dados por parte dos cidadãos, que são os seus detentores.

REFERÊNCIAS

ABRUSIO, Juliana; MARANHÃO, Juliano; CAMPOS, Ricardo; LOPEZ, Nuria. Dados de geolocalização e a investigação do caso Marielle. Revista Consultor Jurídico. 7 de julho de 2020. Disponível em: <https://www.conjur.com.br/2020-jul-07/direito-digital-dados-geolocalizacao-investigacao-marielle?pagina=1> Acesso em mar. 2021

ADEPOL do Brasil e outros. ALERTA GERAL À NAÇÃO SOBRE O NEFASTO ANTEPROJETO DA LGPD PENAL: O FIM DA PREVENÇÃO E REPRESSÃO A CRIMES NO BRASIL. Brasília, 2020. Disponível em: <https://images.jota.info/wp-content/uploads/2020/12/alerta-geral-contra-lgpd-penal-ult.pdf> Acesso em: mar. 2021

ANTEPROJETO de lei disciplina proteção de dados em investigações criminais. Revista Consultor Jurídico, 31 de outubro de 2020. Disponivel em: <https://www.conjur.com.br/2020-out-31/anteprojeto-disciplina-protecao-dados-investigacoes-criminais> Acesso em mar. 2021

ARAS, Vladimir. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. Proteção de dados pessoais e investigação criminal. p. 15. Brasília, 2020.

ARTESE, Gustavo. Privacidade e proteção de dados pessoais: a diluição do consentimento e a responsabilidade demonstrável (accountability). Revista Fórum de Direito na Economia Digital:RFDED, Belo Horizonte, ano 1, n. 1, p. 141-162. Acesso em 5 mar. 2021

ASSOCIAÇÃO NACIONAL DOS PROCURADORES DA REPÚBLICA. Proteção de dados pessoais e investigação criminal /Associação Nacional dos Procuradores da República, 3ª Câmara de Coordenação e Revisão – Brasília: ANPR, 2020. 593 p. ISBN: 978-65-993102-0-1

BARBOSA, Danilo Ricardo Ferreira; DA SILVA, Carlos Sérgio Gurgel. A coleta e o uso indevido de dados pessoais: um panorama sobre a tutela da privacidade no Brasil e a Lei Geral de Proteção de Dados. REVISTA JURÍDICA LUSO-BRASILEIRA, Ano 5 (2019), nº 6, 473-514. Acesso em 6 mar. 2021.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. Lei n. 12.965, de 23 de abr. de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, Brasília, DF, abr. 2014. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: mar. 2021.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD), Brasília, DF, ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: mar. 2021.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74. Acesso em 5 mar. 2021.

BRASIL. Lei nº 13.853, de 8 de jun. de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências., Brasília, DF, jun. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Lei/L13853.htm. Acesso em: mar. 2021.

BUCHNER, Benedikt. Informationelle Selbstbestimmung im Privatrecht. Mohr Siebeck, 2006, p. 41.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Rev. Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. p. 94. Acesso em 6 mar. 2021.

EXCLUSIVO: anteprojeto de lei impõe sigilo sobre dados de investigados, restringe acesso a relatórios do Coaf e dá superpoderes para ANPD. O Antagonista Brasil. 30.10.20. Disponivel em: < https://www.oantagonista.com/brasil/exclusivo-anteprojeto-de-lei-impoe-sigilo-sobre-dados-de-investigados-restringe-acesso-a-relatorios-do-coaf-e-da-superpoderes-para-anpd/> Acesso em 18 mar. 21

FERRAZ JÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito, Universidade de São Paulo, [S. l.], v. 88, p. 439-459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 4 mar. 2021.

FREITAS, Ricardo de Brito A. P. Razão e sensibilidade: fundamentos do direito penal moderno. São Paulo: Juarez de Oliveira, 2001, p. 76.

GALLINATI, Raquel Kobashi, Prado, Tania e Ribeiro, Juliana. LGPD Penal vai dificultar a investigação policial e favorecer a corrupção e a criminalidade organizada. Estadão, Coluna Fausto Macedo. 17 de dezembro de 2020. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/lgpd-penal-vai-dificultar-a-investigacao-policial-e-favorecer-a-corrupcao-e-a-criminalidade-organizada/> Acesso em 18 mar. 21

GUEIROS, Paula M.; MACIEL, A.C.T. A atuação da Autoridade Nacional de Proteção de Dados (ANPD). Migalhas. Brasil, 2021. Disponivel em: <https://www.migalhas.com.br/depeso/341872/a-atuacao-da-autoridade-nacional-de-protecao-de-dados-anpd > Acesso em: 16 mar. 21

LEGAL GROUNDS FOR PRIVACY DESIGN. Instituto Lgpd. 2020. Disponivel em: <https://institutolgpd.com/blog/opal_service/seguranca-publica-e-investigacao-criminal-2/> Acesso em: mar. 2021.

LODDER, George Neves. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: QUESTÕES PENAIS. Associação Nacional dos Procuradores da República Proteção de dados pessoais e investigação criminal. Brasília: ANPR, 2020. p. 132.

MACEDO, Fernanda; BUBLITZ, Michelle e RUARO, Regina. A PRIVACY NORTE-AMERICANA E A RELAÇÃO COM O DIREITO BRASILEIRO. Revista Jurídica Cesumar - Mestrado, v. 13, n. 1, p. 161-178, jan./jun. 2013 - ISSN 1677-64402.

MENDES, Laura Schertel. Privacidade, proteção de dados pessoais e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. (Série IDP: linha pesquisa acadêmica).

_____; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor. Vol. 120, ano 27. Pág. 469-483. São Paulo, Ed. RT, nov-dez 2018. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1116.

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. RJLB, Ano 5 (2019), nº 1.

PARIS. Assembleia Geral da ONU. (1948). "Declaração Universal dos Direitos Humanos" (217 [III] A). Retirado de http://www.un.org/en/universal-declaration-human-rights/. Acesso em: 4 mar. 2021.

PEREIRA, Marcelo Cardoso. Direito à intimidade, proteção de dados e novas tecnologias: em busca de um novo direito. 2011. Disponível em:<http://www.egov.ufsc.br/portal/sites/default/files/anexos/14886-14887-1-B.pdf>. Acesso em: 7 mar. 2021.

QUINTIERE, V. M. Questões controversas envolvendo a tutela jurisdicional penal e as novas tecnologias à luz da Lei Geral De Proteção De Dados (LGPD) brasileira: dataveillance. Revista ESMAT, v. 11, n. 17, p. 175-188, 17 set. 2019.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. Nada a esconder? O direito à proteção de dados frente a medidas de segurança pública e intervenção estatal. Revista Âmbito Jurídico. Cadernos - Direito Administrativo. Brasil, 2011.

_____; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O DIREITO À PROTEÇÃO DE DADOS PESSOAIS E A PRIVACIDADE. Revista da Faculdade de Direito UFPR, Curitiba, v. 53, june 2011. ISSN 2236-7284. Disponível em: <https://revistas.ufpr.br/direito/article/view/30768/19876>. Acesso em: 15 mar. 2021.

_____; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O direito à proteção de dados pessoais e a privacidade. Revista da Faculdade de Direito UFPR, v. 53, 2011.

SILVA, M. R. V. da. A proteção de dados pessoais e seus desafios regulatórios. Revista da Faculdade de Direito, Universidade de São Paulo, [S. l.], v. 114, p. 791-815, 2019. DOI: 10.11606/issn.2318-8235.v114p791-815. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/176613. Acesso em: 5 mar. 2021.

SOLOVE, Daniel J. Introduction: privacy self-management and the consent dilemma. Harvard Law Review, Cambridge, v. 126, p. 1.880-1.903, 2013.

SOMADOSSI, Henrique. O que muda com a Lei Geral de Proteção de Dados (LGPD). Ago 2018. Disponível em: https://www.migalhas.com.br/dePeso/16,MI286235,31047/O+que+muda+com+a+Lei+Geral+de+Protec ao+de+Dados+LGPD. Acesso em: 15 mar. 2021